The Washington
Statewide
Homeland Security Strategic Plan

TEAM WASHINGTON

A statewide collaborative partnership.

2004

✦ Preface ✦

As the Governor's Homeland Security Advisor, I am pleased to provide this copy of the Washington Statewide Homeland Security Strategic Plan. It provides the framework through which we will strengthen our ability to defend against, deter, dissuade and ultimately respond to and recover from terrorist attacks in the State of Washington. It sets the direction and priorities by which we will measure our success in protecting citizens from the dangers that now confront us.

This Strategic Plan is a historic and unprecedented undertaking. We are indebted to the hundreds of private citizens, community and business leaders, tribal representatives, elected officials and federal, state and local government partners whose vision and commitment are reflected in this document. We share a common goal of protecting citizens from the horrific chemical, biological, radiological, nuclear and conventional high yield explosive (CBRNE) threats that have defined the dawn of the 21st Century. We will accomplish this task through effectively coordinating our strategies, tactics, information, technology and other resources, including contingency planning, training and multi-disciplinary/multi-jurisdiction exercises.

As if to underscore the need for this Plan, I am drafting this Preface after a long and exhausting day of coordination with Governor Locke, Department of Homeland Security Secretary Tom Ridge and other state, federal and local leaders. The national Homeland Security Threat Advisory level was increased to Orange (Elevated) this very morning in response to credible information of terrorist plans for an asymmetric attack on the United States.

By following this plan and working together as TEAM WASHINGTON, we will assure our preparedness for such contingencies and fulfill our commitment and responsibility to each other as citizens of this great State and Nation.

Together we will "***Ensure a safe and secure Washington for the 21st Century.***"

Sincerely,

TIMOTHY J. LOWENBERG
Major General
The Adjutant General
Director, Washington Military Department
Washington Homeland Security Advisor

✦ EXECUTIVE SUMMARY ✦

"The liberties of our country, the freedom of our civil constitution, are worth defending against all hazards: And it is our duty to defend them against all attacks."--Samuel Adams

"Ensure a safe and secure Washington for the 21st Century." That is the vision and collective commitment of TEAM WASHINGTON. Terrorist organizations remain committed to death and destruction within our borders. They are targeting our families, our businesses, and our way of life. Protecting Washington State from this campaign of terror requires teamwork. Only by concerted action can we reduce our vulnerabilities and defend against further domestic attacks. Only by strategic planning, training, and exercising can we enhance our collective preparedness. Should terrorists succeed in launching an attack on Washington soil, our response and recovery must be seamless. There is a role within this strategic plan for every person and every organization.

Our statewide homeland security strategic objectives are to:

- Reduce Washington's vulnerability to terrorism.
- Defend against, deter, dissuade and prevent terrorist attacks from occurring within Washington State.
- Prepare citizens, government, tribal nations and businesses at all levels to effectively respond in the event of a terrorist attack.
- Minimize the damage and effectively respond to and recover from attacks that do occur.

Our strategic goals and objectives are based on a foundation of shared values: freedom; community health and safety; economic prosperity and quality of life; security of people, infrastructure and the environment; continuous improvement; financial stewardship and accountability; and an all-citizen and all-state focus in every aspect of executing our strategy.

Washington State has unique challenges and inherent vulnerabilities. We have more than 66,582 square miles of largely remote terrain, a 325-mile international border with Canada, numerous land and maritime border crossings, and 157 miles of open coastline. We have nearly six million people, many of whom live in a Puget Sound corridor of complex waterways and congested roadways. In addition, we have major aerial ports and seaports that are critical components of our state, national, and international transportation industry. We have hundreds of key assets and critical infrastructures, including more than 1,000 dams which in some instances provide power for several other states. We are home to nuclear storage facilities, including the Hanford Reservation and Bangor naval facilities. We are also home to strategic military installations and major national and international business organizations. Our tourist industry also brings in 10 million visitors each year, thereby adding to the population we must protect.

State priorities are to ensure our safety and security by focusing on:

- Fusing and sharing intelligence information among public and private sector entities.
- Enhancing healthcare and public health systems to ensure a surge capacity for emergencies and large-scale disasters.
- Training, equipping, and exercising emergency responders to assure their readiness for complex emergency responses.
- Assessing and protecting key assets and critical infrastructure, including interdependent physical and cyber information systems.
- Planning for and providing continuity of government and business operations before, during and after large-scale disasters.
- Assuring elected officials, community and business leaders, volunteers and citizens are well informed and fully prepared to operate in an emergency environment.
- Protecting and supporting continuous functioning of interoperable communications and public safety information systems.
- Executing proactive deterrence, preemption and prevention initiatives.

The State of Washington and its local partners receive federal funding for initiatives that promote the National Strategy for Homeland Security. In the main, these funds have been restricted to training and equipping emergency responders. Federal assistance has not been available for vulnerability and capability assessments, gap analysis or strategic initiatives. That is why we have focused so heavily on developing this Strategic Plan. We need a clear overarching strategy if we are to address the full spectrum of our state homeland security needs. This Strategic Plan, along with other state and local plans, forms an important foundation for the thoughtful, orderly allocation of resources against domestic security requirements.

✦ TABLE OF CONTENTS ✦

✦INTRODUCTION✦

Terrorists attack vulnerabilities with the intent of weakening the bonds between citizens, businesses, tribal nations, and government at all levels. A terrorist’s goal is to create panic and chaos, disrupting the economy and our American way of life.

It is imperative, therefore, that Washington State execute a strategy that prevents terrorists from exploiting our state. We must develop a “system of systems” that reduces our vulnerabilities and builds a safer and more secure state.

Purpose

The purpose of this plan is to provide an overarching strategy for maximizing our statewide Homeland Security.

Objectives

The statewide homeland security strategic objectives are to:

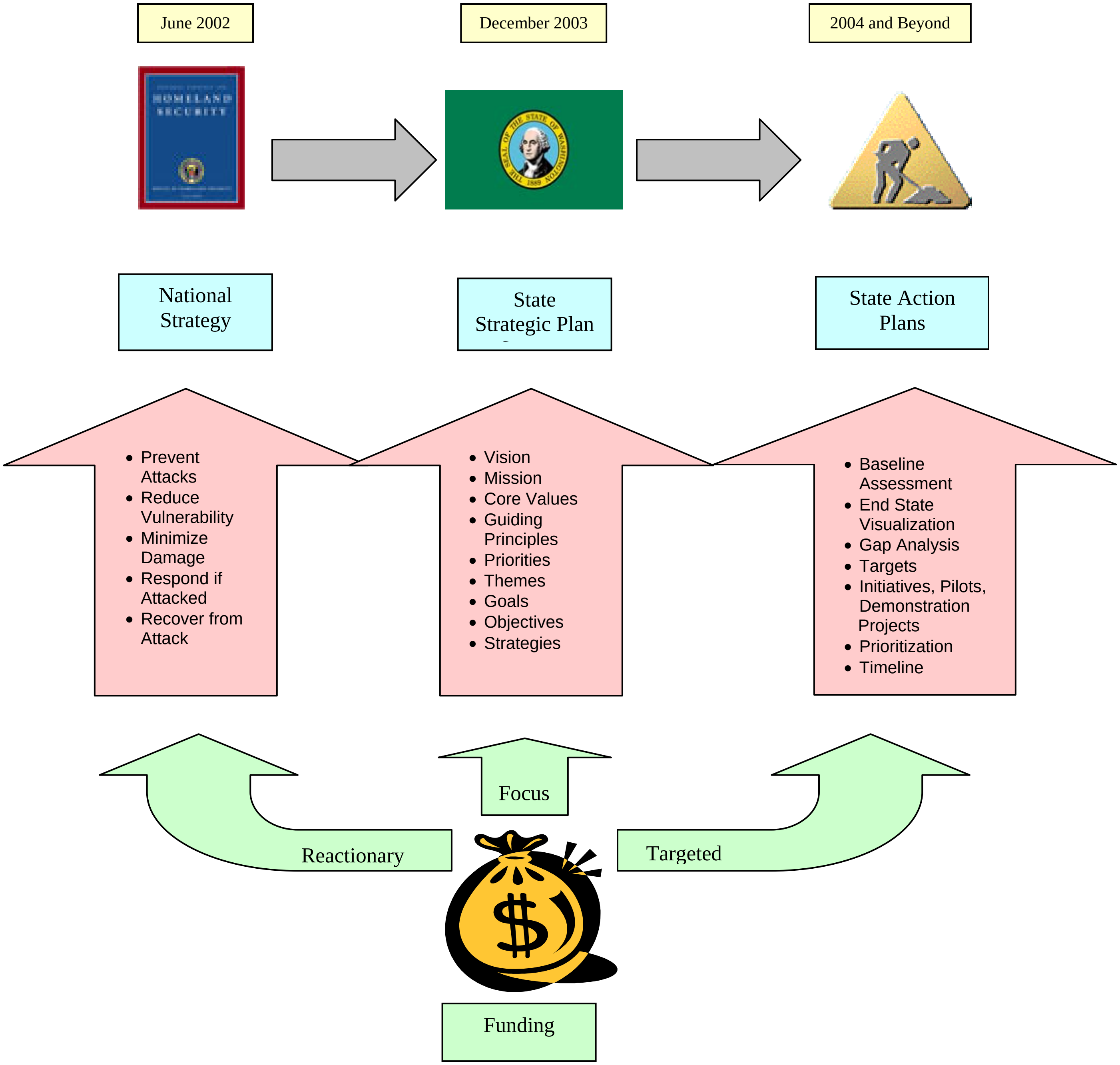
- Reduce Washington’s vulnerability to terrorism.
- Defend against, deter, dissuade and prevent terrorist attacks from occurring within Washington State.
- Prepare citizens, government, tribal nations and businesses at all levels to effectively respond in the event of a terrorist attack.
- Minimize the damage and effectively respond to and recover from attacks that do occur.

Methodology

TEAM WASHINGTON is the statewide collaboration of government, citizens, associations, tribal nations, and public and private sector organizations. This Strategic Plan is the result of extensive interviews, questionnaires, discussions, teleconferences, and meetings with all members of the Team.

The framework shown on the next page was developed to articulate the vision, mission and values used throughout this process. Using this structure, Team Washington’s vision, mission and values were transformed into action through themes, goals and objectives.

Strategic Framework Relationship Diagram



June 2002

December 2003

2004 and Beyond

National Strategy

- Prevent Attacks
- Reduce Vulnerability
- Minimize Damage
- Respond if Attacked
- Recover from Attack

State Strategic Plan

- Vision
- Mission
- Core Values
- Guiding Principles
- Priorities
- Themes
- Goals
- Objectives
- Strategies

State Action Plans

- Baseline Assessment
- End State Visualization
- Gap Analysis
- Targets
- Initiatives, Pilots, Demonstration Projects
- Prioritization
- Timeline

Reactionary

Focus

Targeted

Funding

We receive federal funding for homeland security that is based on the National Strategy. This federal funding model has primarily addressed providing for emergency responder's equipment and training. An evolving process, the state has had to react to a narrowly described and highly regulated system with little opportunity to provide input. The statewide strategic plan determines the full spectrum of the state's homeland security requirements, which will focus funding priorities to build statewide capability and capacity. This strategic plan, as with other state plans, will also illustrate the need to expand grant funding strategies for government at all levels beyond equipping emergency responders to encompass other critical homeland security areas.

The next step in the strategic planning process will include creating action plans that assess where we are, visualize the desired end state, analyze the gaps between vulnerabilities and capabilities, develop targets for closing the gaps, prioritize specific statewide initiatives, implement pilot and demonstration projects and create a timeline for measuring progress in building state capability and capacity - to prevent, prepare for, respond to and recover from a terrorist attack.

The objectives of this process are to develop (1) a framework for measuring performance in critical homeland security mission areas, (2) the ability to make difficult resource allocation decisions, and (3) the flexibility to adjust priorities in light of changing threat conditions.

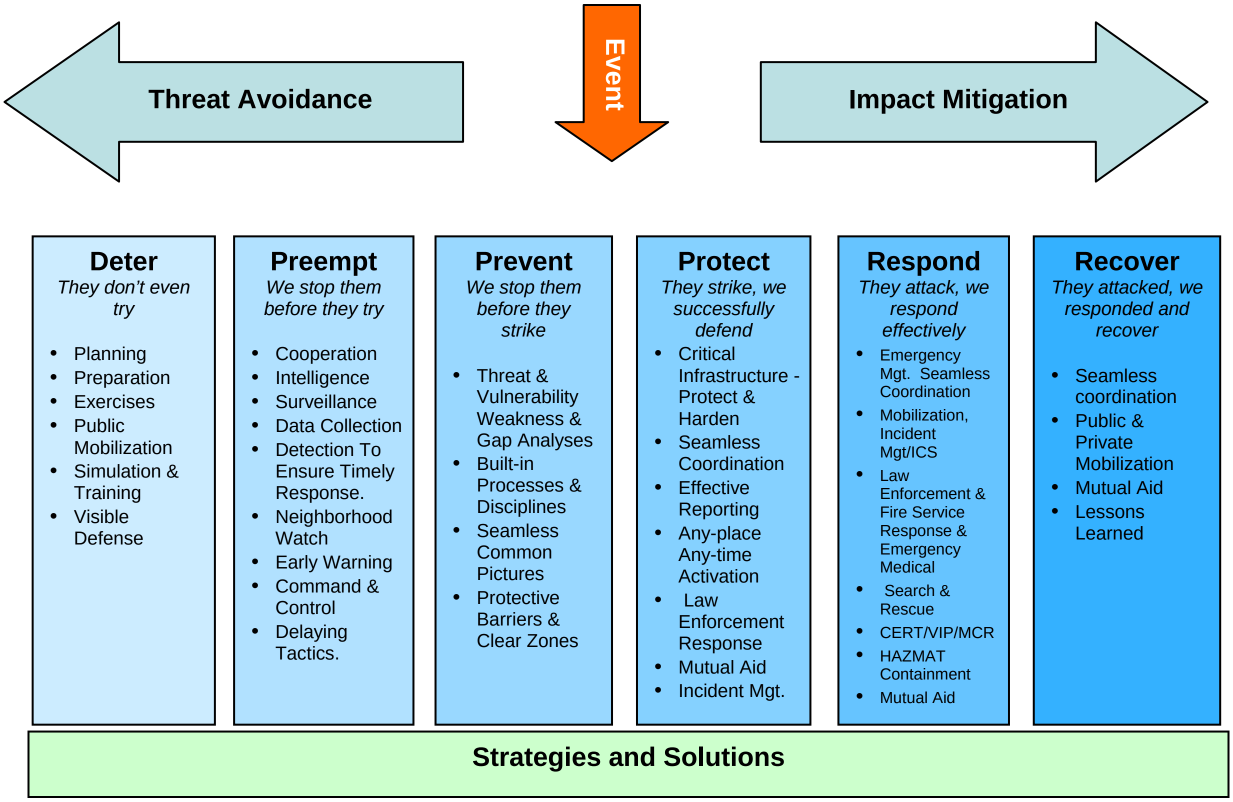
✦ RISK, THREAT, VULNERABILITY ✦

Terrorism can be foreign-state sponsored, organized ideologues, or the outgrowth of frustrated extremists on the fringe of polarized social groups. Terrorists act alone and in highly-dispersed, loose-knit groups.

Washington State is extremely susceptible to terrorist activities. Over the last ten years there have been numerous documented terrorist threats, extremist group activities, and terrorist cells operating within our borders. The threats and events included conventional weapons, improvised or high-yield explosive devices, bioterrorism hoaxes, and attempted cyber attacks.

The homeland security threat spectrum diagram below identifies the components of a possible act of terrorism to include threat avoidance, the actual event, and impact mitigation. The statewide strategy addresses all aspects of the threat spectrum to include a developing framework for the prevention of terrorism and improving our ability to respond rapidly to restore normalcy, thereby preventing a terrorist from “succeeding” in attempt to harm Washington state interests.

HLS Threat Spectrum



Threat Avoidance

Event

Impact Mitigation

Deter
They don't even try
- Planning
- Preparation
- Exercises
- Public Mobilization
- Simulation & Training
- Visible Defense

Preempt
We stop them before they try
- Cooperation
- Intelligence
- Surveillance
- Data Collection
- Detection To Ensure Timely Response.
- Neighborhood Watch
- Early Warning
- Command & Control
- Delaying Tactics.

Prevent
We stop them before they strike
- Threat & Vulnerability Weakness & Gap Analyses
- Built-in Processes & Disciplines
- Seamless Common Pictures
- Protective Barriers & Clear Zones

Protect
They strike, we successfully defend
- Critical Infrastructure - Protect & Harden
- Seamless Coordination
- Effective Reporting
- Any-place Any-time Activation
- Law Enforcement Response
- Mutual Aid
- Incident Mgt.

Respond
They attack, we respond effectively
- Emergency Mgt. Seamless Coordination
- Mobilization, Incident Mgt/ICS
- Law Enforcement & Fire Service Response & Emergency Medical
- Search & Rescue
- CERT/VIP/MCR
- HAZMAT Containment
- Mutual Aid

Recover
They attacked, we responded and recover
- Seamless coordination
- Public & Private Mobilization
- Mutual Aid
- Lessons Learned

Strategies and Solutions

Washington State has unique challenges and key potential targets that contribute to the state's vulnerability. Washington's geography, over 66,582 square miles of largely remote terrain, a 325-mile international border with Canada with several border crossings, and 157 miles of coastline, complicates the ability to protect the state. Most of the state's nearly 6 million people live in a relatively small corridor in Puget Sound that has complex waterways and congested traffic arterials. The state enjoys a large tourism industry of over 10 million visitors annually that adds to the complexity of ensuring a secure state. In addition, there are heavily utilized air and sea ports for state, national and international transit. The state is also home to several key energy assets to include over 1,000 dams with major power facilities supporting several other states. Washington State houses nuclear storage facilities to include the Hanford Reservation, and Bangor facilities. Many important military installations are within Washington's borders, and we are home to many prominent national and international businesses.

Many of Washington's communities are vulnerable to terrorist incidents and several have highly visible and vulnerable targets. These critical facilities, sites, systems, and special events are often located near routes with high transportation access.

The following list identifies some of the state's major critical infrastructure sectors:

- **Agriculture and Food** – Agriculture and related industries account for nearly 13 percent of the annual gross state product. The state has approximately 37,000 farms producing over 300 commercial crops with a farmgate value of over $5.5 billion. Washington is the number one state in the United States for apples, red raspberries, corn for processing, concord grapes, sweet cherries, pears, tart cherries, lentils and hops; we rank number two nationally for asparagus, processing peas, dry peas, apricots, fall potatoes and all grapes; and we are number three in the country for dry onions, trout, wheat, prunes, and plums. Agriculture and food includes supply chains for feed, animals and animal products; crop production and the supply chains of seed, fertilizer, and other necessary related materials; post-harvesting components of the food supply chain from processing, production, and packaging through storage and distribution to retail sales, institutional food services, and restaurant or home consumption.

- **Water** – Washington State has over 8,000 lakes and 40,000 rivers and streams to protect. Our water infrastructure is made up of both fresh water supply and wastewater collection and treatment. The protection of water and waste systems is vital fighting fires, providing clean water for public health and safety, and maintaining a secure water supply for hospitals and for our overall state economic viability.

- **Healthcare and Public Health** Key to sustaining the health of our almost 6 million residents, is the healthcare and public health sector that is made up of state and local health departments, hospitals, health clinics, mental health facilities, nursing homes, blood-supply facilities, laboratories, mortuaries, pharmaceutical stockpiles, and veterinary services. While there are literally thousands of licensed facilities, the state public health system is directed by the state Department of Health and 35 local health departments/districts. The healthcare system is composed of 96 licensed and 102 rural health clinics.

- **Emergency Services** – Washington State has over 100,000 emergency responders: fire, rescue, emergency medical services, 9-1-1, law enforcement, and emergency management personnel that are vital to assuring our state's critical homeland security capabilities.

- **Government Facilities** – Within Washington State there are major Army, Navy, Air Force, and Coast Guard facilities. These bases are strategically located to support and deploy forces worldwide providing employment to over 100,000 civilian and military employees in the state.

  There is also a great deal of other federal government infrastructure in Washington State that is vital to state and national security. Washington is home to the FEMA Region X Headquarters, the Federal Reserve Regional Headquarters, Federal Courthouses, FAA facilities and many other important entities.

  The state government owns almost 11,000 buildings and employs over 102,000 people. In addition, local governments protect and secure 39 county jurisdictions and over 281 cities.

  Public education is a key component of our governmental capabilities with nine Educations Service Districts (ESDs), three independent districts, and 296 state school districts with over 2200 school buildings. In addition to being vital state resources that must be protected, schools provide significant resources for emergency response and recovery facilities as command centers, staging areas, and recovery operations centers.

- **Defense Manufacturing Capability** - The "defense industrial base" refers to the support systems and capability of industry to produce essential material to support national military objectives -- e.g., repair parts, ammunition, chemical defense supplies, food, medical, and fuel supplies. Within Washington's borders there are numerous defense contractors producing critical military equipment systems and supplies.

- **Information and Telecommunications** - Voice and data services are vital to business operations and for keeping citizens connected to government and one another. This critical infrastructure sector affects every resident because of the complex interdependencies and the magnitude of telecommunications and cyber systems within Washington.

- **Energy** – Electricity generating plants in Washington have a total installed capacity of 24.2 million kilowatts and produce approximately 100.5 billion kilowatt hours of electricity each year. Washington leads the nation in both installed capacity and annual production of hydroelectricity. The system of dams in the state is the key to this capacity. Approximately 87 percent of the annual output of electricity is produced by hydroelectric facilities, about seven percent by conventional thermal installations, and about six percent by nuclear power plants. This sector includes electricity generating dams, power plants, transmission and distribution systems; oil production, crude oil transport, refining, product transport and distribution, and control and other external support systems; and natural gas exploration and production, transmission, and local distribution.

- **Transportation** – The state transportation infrastructure has aviation, maritime, rail, bridges, highways, trucking, busing, pipelines, and mass transit systems. There is a robust transportation system in Washington State built upon a network of 81,300 miles of federal, state, and local roads, including the nation's largest fleet of ferries. The state is also served with about 2,075 route miles of Class I railroad track and 1,115 miles of track operated by 17 short-line railroads, and two Amtrack Cascade trains. Washington has 76 public port districts. The combined ports of Seattle and Tacoma are the second largest container load centers in the United States. Agricultural commodities and other goods are also transported throughout Puget Sound and river systems. Washington has 127 public airports, three seaplane bases, Seattle-Tacoma and Spokane International Airports, and a number of regional transportation airports.

- **Banking and Finance** – Herein are included; physical banking and financial structures, financial utilities and human capital, wholesale banking operations, financial markets, regulatory institutions, physical repositories for documents and financial assets. Washington State has an extensive financial community with depository institutions and trust companies of over $102 billion in assets, over 100,000 firms/individuals providing securities investments and advice representing over $579 billion statewide, $5 billion in real estate secured loans and over $879 million in short term in-state loans for the year 2002, as an example. The state also has a $19 billion statewide insurance industry with over 1,374 insurance companies with 50 domestic insurers with headquarters in the state.

- **Chemical Industry and Hazardous Materials** - The use of chemicals is a fundamental component of Washington State industry and infrastructure. The manufacture and distribution of chemicals occur on a daily basis and are required for all aspects of business and daily life. Each year businesses report the storage, processing, and planned and unplanned releases via reports to the State Emergency Response Commission as required under the Emergency Planning & Community Right-to-Know Act. For FY 2002, approximately 3,500 businesses reported 14,766 chemicals and products stored at 24,915 sites throughout Washington State. In addition, 355 facilities report over 1,173 chemicals via the Toxics Release Inventory Report submitted to the SERC and the EPA in a typical year. In addition to tracking the hazardous chemicals, the reported data includes 3,421 extremely hazardous substances which pose the greatest threat to human health and safety for the citizens of Washington State. Washington also houses approximately 7,000 hazardous waste generators that produce more than 255 million pounds of hazardous waste annually. These chemical products and waste are transported through major population centers on Washington State highways, rails and waterways. The combined quantity of manufactured, processed, transported, and stored hazardous chemicals presents a significant threat to the citizens of Washington State. The threat of harm from a hazardous chemical release is present whether the release is accidental or an act of terrorism. In addition, the Washington State Poison Center maintains the complex mission of providing information on 47 million chemicals and responds to over 100,000 inquiries per year in support of public health and safety.

- **Postal and Shipping** - Washington State is home to several key air, sea and inland ports that are vital in the intermodal movement of cargo regionally, nationally and internationally. Washington has the largest controlled public port system in the world with 76 ports that have interests including marine terminals, barge facilities, industrial development, fuel depots, marinas airports, railroads and military cargo. The Ports of Tacoma and Seattle are Washington's largest seaports and combined they make up the 3rd largest U.S. load center behind Los Angeles/Long Beach and New York/New Jersey. The Ports of Tacoma and Seattle import and export millions of containers with goods ranging from agriculture products to electronic equipment. Seattle has a large and growing cruise business while Tacoma is one of thirteen power projection platforms in the US that are vital to military bases such as Fort Lewis. Washington ports handle 7 percent of all U.S. exports and 6 percent of all imports representing in excess of $100 billion of trade annually and contributing to the state economy by creating one out of every four jobs in the Washington State.

- **Key Assets** Historical attractions, monuments, cultural centers, nationally prominent companies, commercial centers, sports stadiums, schools, universities, and parks and recreation are among the many key assets in Washington State.

Critical facilities and special events become more vulnerable during dignitary visits, international meetings, conventions, and major media events. Sporting events such as the World Series, Super Bowl, Basketball Championships, World Cup, and Olympic Games provide excellent environments for terrorists to broadcast their causes through violence. Terrorists will go to great lengths to ensure that an event produces the intended impact, even if it means destroying an entire structure or killing thousands of victims.

Terrorists use many conventional means to achieve their objectives. Of greatest concern, however, is the use of weapons of mass destruction. Experts generally agree that there are five categories of terrorist incidents: chemical, biological, radiological, nuclear, and explosive (CBRNE).

Chemical agents are potentially lethal, relatively inexpensive, and easy to produce. Washington hosts an extensive, legitimate chemical product industry with products that can be used as terrorist weapons. A chemical attack is defined as the deliberate release of a toxic agent (gaseous, liquid, or solid) that can poison people or the environment. The effects of chemical agents absorbed through the skin or mucous membranes are usually immediate, obvious and will require rapid mobilization of all levels of emergency responders. Readily available, these weapons have been used in terrorist acts such as the Aum Shinrikyo cult 1995 Tokyo subway incident.

Biological agents are also lethal, accessible, capable of being weaponized for mass dissemination of small-particle aerosols, and the effects may not be immediately known, giving the infectious agent time to rapidly spread. Many biological agents can be adapted by terrorists and released into a population or environment. Potential foreign nation stockpiles create a possible source of biological material for terrorists. A biological incident will most likely be recognized in a hospital emergency room, medical examiner’s office, or within the public health community long after the terrorist attack. Biological outbreaks require rapid procurement and mass distribution of drugs and vaccines to treat, contain and avoid mass casualties and panic.

Radiological weapons or “dirty bombs” combine radioactive material with conventional explosives to create a non-nuclear dispersion device. Radioactive materials range from highly controlled uranium or plutonium to low grade materials commonly used to treat illness, sterilize equipment, inspect welding seams, and irradiate food. The force of the explosion and radioactive contamination will be more localized than in a nuclear blast. The presence of radiation may not be detected until trained personnel with specialized equipment are on the scene. With limited exposure, it is unlikely that radioactive materials contained in a dirty bomb would result in serious health effects or death. Injury or death would likely occur from the explosion itself.

Nuclear threats include the actual detonation of a nuclear bomb or device. Detonation of a nuclear device would produce high temperatures, sharp increases in atmospheric pressure, flying debris, and radiation emissions. Injuries could include massive trauma, burns, blunt and puncture wounds, fractures, lacerations, flash blindness, scarring of the retinas and radiation exposure. A nuclear attack would create a public health crisis calling for immediate treatment and subsequent fallout responses.

Explosive incidents account for 70 percent of all terrorist attacks worldwide. Incendiary devices are mechanical, electrical, or chemical devices used to intentionally initiate combustion and start fires. The Internet and local libraries provide ample information on the design and construction of explosive devices. Targets range from small gatherings (suicide bombers) to structures containing thousands of people (vehicle bombs). These devices may be used singularly or in combination and can cause death, injury and chaos within our communities. Additionally manufacturing activities often involve hazardous materials that have a potential for misuse by terrorists as explosives. Equally dangerous is the explosive potential of terrorist acts against shipping of hazardous materials such as fuels and other flammable products.

Cyberterrorism is a relatively new method of attack that can seriously disrupt our society and exploit our reliance on computers and telecommunication networks. Cyberterrorism threatens the electronic infrastructure supporting the social, health, and economic well being of Washington's citizens. Interlinked computer networks regulate the flow of power, water, financial services, medical care, telecommunication networks, and transportation systems. These networks are vulnerable to attack and it is difficult to distinguish a singular hacker-type incident from a cyber-terrorist attack or to determine the source of an attack. The tools for conducting cyberterrorism are widely available, broadly advertised, and easily used. The consequences can be quite severe causing chaos, panic, disruption of operations and economic losses.

Agriterrorism is the malicious use of plant insect pests or pathogens or animal pathogens to cause devastating damage in the agricultural sector. Anti-livestock pathogens are of the greatest concern because they can be introduced relatively easily and spread quickly. The insect pests and plant pathogens designed to attack existing crops are thought to be less effective weapons because they spread slowly and unreliably and are highly influenced by weather. It would be difficult to cause the widespread destruction of a crop because most crops are not grown in isolation and have already been exposed to many pathogens, thereby increasing their resistance to infection. The infection of seed may also be a source of introduction. There are several factors that increase the state and nation's vulnerability to agriterrorism: 1) there are many agents that are lethal and highly contagious to animals, many of which we do not vaccinate against, 2) many of these agents are non-zoonotic and can be transported by a terrorist without any special personal precautions or training, 3) antibiotic and steroid programs and husbandry programs designed to improve quality and quantity of meat have made U.S. livestock more susceptible to exotic disease, 4) animal populations are highly concentrated, and large herds make ideal targets for infection and contagion, 5) animal populations are highly mobile creating conditions where animals that are incubating disease during movement can increase the spread of disease, 6) agricultural facilities are not highly secure, and the U.S. currently has limited detection capabilities. The main impacts of an agriterrorism attack would be the economic impact of agricultural losses and subsequent impacts to our economy. One in eight jobs nationally depends on food production. In addition, a successful agriterrorism attack would undermine confidence in our ability to protect the citizens of this country.

These terrorist methods are not all-inclusive and are constantly evolving. Our adversaries seek to remain invisible and strike targets of opportunity that achieve maximum attention and impact. We must therefore create and sustain a high level of readiness.

✦ VISION STATEMENT✦

Ensure a safe and secure Washington for the 21st Century.

✦ MISSION STATEMENT✦

To protect the citizens, property, environment, culture and economy of Washington State from acts of terrorism and to minimize the effects of a terrorist attack.

✦ CORE VALUES ✦

- **Freedom**
- **Community Health and Safety**
- **Economic Prosperity and Quality of Life**
- **Security – Protect People, Infrastructure and the Environment**
- **Teamwork – All-Citizen and All-State Focus**
- **Continuous Improvement**
- **Ethical Relationships and Management**
- **Financial Stewardship and Accountability**

✦ GUIDING PRINCIPLES ✦

- Homeland security is every citizen’s responsibility.
- Prevention through an empowered, educated and vigilant citizenry.
- Enhance response capability through planning, equipping, training and exercising.
- Build core statewide capabilities and augment resources based on assessed threats and vulnerabilities.
- Achieve safe and effective protections through standardization and interoperability.
- Capacity, once created, must be supported and sustained into the future.
- Washington State will be secure only when our communities are secure.

“Our challenge is to build new barriers to terrorists and new bridges to one another.”
DHS Secretary Tom Ridge Oct 2003

✦ STRATEGIC HOMELAND SECURITY PRIORITIES ✦

- Fusing and sharing intelligence information among public and private sector entities.

- Enhancing healthcare and public health systems to ensure a surge capacity for emergencies and large-scale disasters.

- Training, equipping, and exercising emergency responders to assure their readiness for complex emergency responses.

- Assessing and protecting key assets and critical infrastructure, including interdependent physical and cyber information systems.

- Planning for and providing continuity of government and business operations before, during and after large-scale disasters.

- Assuring elected officials, community and business leaders, volunteers and citizens are well informed and fully prepared to operate in an emergency environment.

- Protecting and supporting continuous functioning of interoperable communications and public safety information systems.

- Executing proactive deterrence, preemption and prevention initiatives.

✦ STRATEGIC THEMES✦

Strategic themes are part of the framework that translates the statewide vision, mission and values into action. Themes dissect the strategic priorities and organize them into topic areas in which we must excel if we are to accomplish our homeland security mission and vision. Themes support the state's core values:

- **Partnership and Leadership**

  Promote a collaborative environment for sharing information, resources, assistance, and expertise as we jointly strive to enhance our security environment.

- **Communication**

  Interoperable systems that provide critical information in a timely fashion to those who need it and in a form that is easy to use and understand.

- **Prevent Attacks**

  A wide spectrum of prevention efforts including intelligence and warning capabilities to ensure joint situational awareness, border security, domestic counterintelligence, and hardening of critical infrastructure.

- **Reduce Vulnerabilities**

  Protect our way of life by improving the protection of the individual pieces and interconnecting systems that make up our critical infrastructure (e.g., economy, agriculture, food water, public health, emergency services, government, defense manufacturing capability, information and telecommunications, energy, transportation, banking and finance, chemical industry, postal and shipping).

- **Emergency Preparedness/Response - Education & Training**

  "Trained, Equipped and Exercised = A Ready Washington State." Provide effective and comprehensive education for all emergency responders, emergency managers, citizens, volunteers, tribal nations, government, and private sector entities.

- **Emergency Response & Recovery - Minimize Damage & Recover from Attacks**

  The statewide objective is to minimize damage and recover rapidly from any attacks that may occur. Efforts will continue to encompass an all-hazards approach that is integrated into statewide emergency management.

- **Resource Capacity**

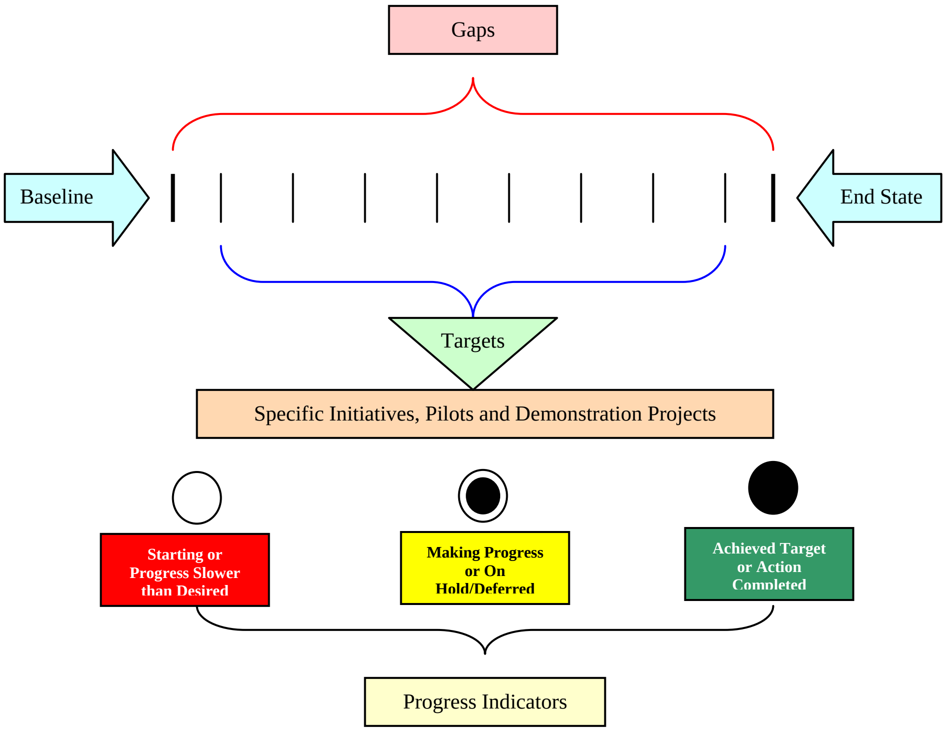
  Homeland security resources are limited. There is a shared responsibility to fund and ensure wise stewardship of scarce resources that synchronizes with our goals and objectives and builds long-term sustainability.

✦ STRATEGIC GOALS ✦

Strategic planning is normally conducted for a single organization. Homeland security strategic planning is conceptual in nature and must integrate many sectors of society.

For all goals, objectives, and strategies we will partner as a statewide community with government at all levels, tribal nations, the private sector, associations, organizations, and citizens to ensure a safe and secure state for our residents. The matrix presented on the following pages outlines our goals, objectives, and strategies which are part of the strategic planning framework linkage that transforms the statewide vision and mission into action. Goals represent what we must achieve within each theme/perspective in order to achieve the vision and mission. Objectives further define goals into specific steps or end states for goal accomplishment. Strategies define what must be done to accomplish the goals that support our mission and vision within each thematic area.

The action planning framework shown below is the next phase of our strategic planning process. Each action plan starts with an assessment of the goals, objectives and strategies to determine a statewide baseline. Next will be a visualization of the desired end state. Gap analysis will be employed for developing targets. Each target will detail specific initiatives. A prioritization of initiatives will determine those areas with the greatest opportunity to build needed statewide capacity and capability. Progress will be measured for each action plan. The lead responsible entities for these task oriented action plans and timelines will be part of the action plan.


Gaps
Baseline
End State
Targets
Specific Initiatives, Pilots and Demonstration Projects
Starting or Progress Slower than Desired
Making Progress or On Hold/Deferred
Achieved Target or Action Completed
Progress Indicators

For use throughout this strategic plan: the "National Strategy for Homeland Security" defines "State" to be "any state of the United States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, the Canal Zone, the Commonwealth of the Northern Mariana Islands, or the trust territory of the Pacific Islands." The Strategy defines "local government" as "any county, city, village, town, district or other political subdivision of any state, any Native American tribe or authorized tribal organization, or Alaska native village or organization, and includes any rural community or unincorporated town or village or any other public entity for which an application for assistance is made by a state or political subdivision thereof."

Ensure a safe and secure Washington for the 21st Century.

Goal	Objectives	Strategies
PARTNERSHIP & LEADERSHIP		
To engage statewide partners to ensure homeland security interests are understood and supported.	1.1 Define statewide Homeland Security interests, roles, responsibilities and structure.	1.1.1 Further develop partnerships to identify existing capabilities and capacities to meet the threat of terrorism and ensure there are clear linkages between all levels of government, tribal nations, private sector and citizens. 1.1.2 Review the existing statewide domestic security structure to maximize the organizational efficiency and effectiveness.
	1.2 Review existing and proposed laws to ensure synchronization with local/state government and tribal nations homeland security goals and objectives.	1.2.1 Develop and maintain an effective system to ensure state laws support homeland security preparedness, prevention, response and recovery requirements. 1.2.2 Monitor state and national legislation for homeland security impact and maintain a dialogue with state and federal legislators to ensure statewide interests are considered.
	1.3 Refine statewide continuity of government and continuity of service plans to ensure essential functions in case of a disaster.	1.3.1 Review existing plans. 1.3.2 Develop, where necessary, detailed planning for continuity of government and critical services within the state.
	1.4 Create action plans to lead the statewide effort to prioritize initiatives, and projects to build homeland security capability and capacity.	1.4.1 Create task oriented action plans that include establishing a baseline, desired end states, targets and performance measures for the statewide goals and objectives.
	1.5 Build a strong and engaged partnership between federal, state and local government, tribal	1.5.1 Partner with business, all levels of government and statewide associations to improve emergency capabilities and capacity. 1.5.2 Include the business community in the state Emergency Operations Center operations to ensure a strong partnership during disaster operations.

Ensure a safe and secure Washington for the 21st Century.

Goal	Objectives	Strategies
	nations, special purpose districts and the private sector to facilitate building state homeland security capability and capacity.	1.5.3 Include the business community in the statewide domestic infrastructure membership. 1.5.4 Explore the best ways to communicate and educate the business community for homeland security.
COMMUNICATION		
To facilitate statewide communication and collaboration.	2.1 Ensure interoperability for communications equipment, networks and advisory systems to achieve statewide communications capability.	2.1.1 Define statewide interoperability standards and inventory statewide systems in collaboration with the State Interoperability Executive Committee (SIEC). 2.1.2 Resolve interoperability gaps, including both voice and data capability.
	2.2 Define communications protocols and methodology to ensure statewide connectivity.	2.2.1 Establish a homeland security communications plan for both secure and non-secure means to communicate internally and externally with local, state and federal partners. 2.2.2 Maintain effective scalable statewide communication networks to educate, share information and emergency procedures and provide advisories. 2.2.3 Maintain and improve the Homeland Security Advisory System (HSAS). Continue to dialogue with state and federal partners to identify and resolve system issues. 2.2.4 Develop a Homeland Security Public Information Plan.
	2.3. Define the need and circumstances for formal coordination agreements between agencies (public and private) describing mechanisms to exchange and share information.	2.3.1 Develop information sharing templates for agreements and parameters for exchange of information.
	2.4 Ensure statewide information sharing and communications systems are protected from threats.	2.4.1 Refine and develop where necessary effective cyber prevention and preparedness capability and capacity to protect the integrity and continuity of statewide information sharing and communication systems.

Ensure a safe and secure Washington for the 21st Century.

Goal	Objectives	Strategies
PREVENT ATTACKS		
To understand, detect and respond to threats.	3.1 Develop and implement terrorism monitoring, threat assessment, and information sharing systems.	3.1.1 Partner regionally and nationally to develop and implement effective systems for terrorist threat monitoring and surveillance.
		3.1.2 Define the essential elements of critical homeland security information.
		3.1.3 Establish a system for dissemination of all relevant terrorism data and information to ensure reliable capability to alert officials and emergency response personnel of terrorist threats statewide.
		3.1.4 Establish a statewide prevention information, analysis, and intelligence sharing and infrastructure protection capability.
		3.1.5 Integrate daily use systems used in emergency response coordination into the information collection and dissemination system.
		3.1.6 Create a central antiterrorism intelligence and analytical center [(Washington Joint Analytical Center – (WAJAC)].
		3.1.7 Establish one additional regional intelligence group; strengthen capacities and capabilities of existing groups.
	3.2 Coordinate statewide for prevention plans, assessments, procedures, infrastructure protection and funding priorities.	3.2.1 Use the state homeland security structure to coordinate and facilitate the building prevention capacity.
	3.3 Adopt or develop an appropriate analytical “risk management” model to assess risk or vulnerability and identify methods to reduce risk.	3.3.1 Establish threat reduction “anti-terrorism” activities, assist and educate the private sector.
	3.4 Improve threat recognition to halt the development of a terrorism threat before it is executed.	3.4.1 Create a system to regional system capability that consists of a fully computerized file system that is integrated between regions; system capability should include analytical software and GIS imagery with law enforcement database sharing to collect, screen, and store relevant information with prevention investigative value..
		3.4.2 Map threats and capabilities for preemptive action.
		3.4.3 Explore the use of remotely sensed Geographic Information Systems (GIS) data in the effort to map statewide threats.
		3.4.4 Establish a public and private community based pre-incident

Ensure a safe and secure Washington for the 21st Century.

Goal	Objectives	Strategies
		“threat indicator” training program.
	3.5 Improve the northern border area security.	3.5.1 Define roles and responsibilities and work on actions to improve the northern border area security.

REDUCE VULNERABILITIES

Goal	Objectives	Strategies
To reduce Washington State’s vulnerability to acts of terrorism.	4.1 Protect critical infrastructure within Washington State.	4.1.1 Define criteria and identify statewide critical infrastructure.
		4.1.2 Conduct statewide critical infrastructure assessments.
		4.1.3 Develop threat detection capabilities for critical infrastructures.
		4.1.4 Develop countermeasures to protect critical infrastructures.
	4.2 Create a statewide critical infrastructure mapping system.	4.2.1 Utilize mapping capability to map critical infrastructure so that information is available to analyze infrastructure geospatial interrelationships.

EMERGENCY PREPAREDNESS/RESPONSE - EDUCATION & TRAINING

Goal	Objectives	Strategies
To improve statewide emergency preparedness and readiness.	5.1 Equip, and train emergency responders to nationally recognized standards.	5.1.1 Identify equipment standards, priorities, shortages and funding needs for emergency responders.
		5.1.2 Develop a multi-discipline training capability to provide statewide emergency responders training, certification, and credentialing –Homeland Security Institute (HSI).
	5.2 Focus exercises to strengthen homeland security critical mission areas concentrating on the complete homeland security threat spectrum (deter, preempt, prevent, protect, respond and recover).	5.2.1 Develop, plan and exercise for WMD preparedness certification. Incorporate emergency responders, private industry, state and local government, tribal nations, federal partners and volunteers in exercises to enhance statewide response capability.
		5.2.2 Develop a broad based exercise program to leverage existing resources and systems.
		5.2.3 Use NIMS/ICS in state and local exercises and real world events.
		5.2.4 Develop and exercise mutual assistance compacts.
	5.3 Train and educate citizens, volunteers, tribal nations, the business community, the media and government on terrorism.	5.3.1 Develop public education, training and information programs.
		5.3.2 Develop and disseminate training materials, templates on how to prepare for, recognize, report, and respond to a threat or act of terrorism.
		5.3.3 Train and exercise elected state and locally appointed officials to ensure competency in Incident Management and Continuity of Government operations.

Ensure a safe and secure Washington for the 21st Century.

Goal	Objectives	Strategies
		5.3.4 Develop a state-wide NIMS Incident Command System (ICS) education and training program.
		5.3.5 Publicize the Homeland Security Advisory System and the guides for preparedness statewide.
	5.4 Enhance our public health and healthcare capabilities to respond to chemical, biological, radiological, nuclear, and explosive terrorism incidents.	5.4.1 Train and educate health care professionals from all sectors to respond as part of the statewide medical response capability.
		5.4.2 Optimize regional medical surge capacity for victims of terrorism through concentrated needs assessment, and planning to eliminate gaps.
		5.4.3 Build statewide chemical/bioterrorism capability by expanding laboratory capacity, enhancing continued disease preparedness activities, urgent disease reporting capability, and education, training exercises and drills.
		5.4.4 Build statewide containment and isolation capacities to respond to chemical and bioterrorism attacks.
		5.4.5 Build hospital decontamination capabilities and capacity statewide.
	5.5 Use lessons learned and best practices to improve disaster resistance.	5.5.1 Research best practices in other states, and pursue partnership and pilot project opportunities.
		5.5.2 Utilize and/or conduct after action reviews for exercises, training, planning sessions and other opportunities.
		5.5.3 Document and share lessons learned to help build our mutual strength and knowledge.
	5.6 Build the state volunteer citizen capability and capacity.	5.6.1 Provide training through local, state and federal programs or other resources for volunteer groups to increase knowledge and group proficiency to better support emergency responders.
		5.6.2 Promote and publicize volunteer opportunities to the public.
	5.7 Exploit information systems and cyber technologies to enhance statewide preparedness and response.	5.7.1 Utilize building mapping capability to map our critical infrastructure so that information is available to all state, local, federal, tribal and private emergency responders.
		5.7.2 Create a secure, portable information technology system emergency responders can utilize to facilitate incident command and management of key resources, identify and track credentialing, schedule on-site resources, locates required resources, tracks casualties and plans on-scene.
	5.8 Enhance regional CBRNE response capability and capacity statewide.	5.8.1 Support and sustain existing regional CBRNE response capability and capacity statewide.
		5.8.2 Establish and sustain regional Hazardous Materials (HAZMAT) response capability and capacity statewide.

Ensure a safe and secure Washington for the 21st Century.		
Goal	**Objectives**	**Strategies**
EMERGENCY RESPONSE & RECOVERY - MINIMIZE DAMAGE & RECOVER FROM ATTACK		
To enhance our statewide system to minimize damage and ensure rapid response, and recovery from a terrorist attack.	6.1 Build state and local Incident Management team capabilities.	6.1.1 Define and identify Incident Management Team concepts, membership, capabilities, responsibilities and training needs at the state and local level.
	6.2 Manage the logistics of emergency resources to maximize response and recovery capability.	6.2.1 Enhance capability to receive, store and distribute emergency response stockpiles (e.g.., Strategic National Stockpile.), implement the Prepositioned Equipment program, and coordinate EMAC resources. 6.2.2 Develop and maintain a state-wide logistics resource database for equipment and supplies to include available assets from all sectors. 6.2.3 Review emergency purchasing and acquisition plans to ensure equipment and supplies can be quickly procured in a disaster. 6.2.4 Review and enhance disaster mortuary plans and capabilities.
	6.3 Improve recovery planning, resourcing, training and exercises capability and capacity.	6.3.1 Review statewide recovery capability and capacity and enhance where necessary. 6.3.2 Include recovery tasks in annual exercises and training objectives. 6.3.3 Develop victim assistance plans (e.g., special needs population, mental health issues, and orphans) for potential terrorist events.
RESOURCE CAPACITY		
To build long-term financial stability, capacity and capability.	7.1 Coordinate statewide to ensure effective and efficient investment in the state's homeland security requirements.	7.1.1 Identify funding opportunities to augment homeland security efforts. 7.1.2 Coordinate statewide to reduce duplication of effort and resources.
	7.2 Make interoperable acquisition decisions for homeland security investment.	7.2.1 Focus acquisition strategies to achieve statewide interoperability. 7.2.2 Develop a core statewide emergency response capability and then augment based on threat.
	7.3 Invest based on statewide homeland security priority list.	7.3.1 Develop and maintain a state homeland security priority list to fund when resources are available.

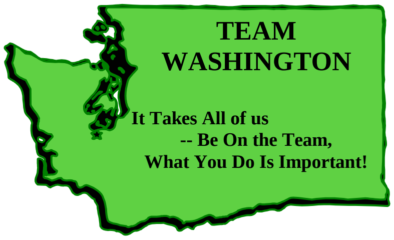
✦ CONCLUSION✦

Washington strives to build terrorism capabilities and capacities that are integrated into the State's all hazard emergency management strategy and that can be sustained long term. Much has been done to counter the ongoing threats of terrorism through increased planning, equipping, training, and exercises. In addition, our statewide security continues to improve through enhancing regional coordination, educating and engaging our citizenry, strengthening existing partnerships and forming new, collaborative relationships.

Washington State will focus its attention on the priorities in this strategic plan and continue to work with local, state and national partners. This strategic plan will help determine the State's homeland security requirements, thereby enabling us to focus resources and maximize our counter-terrorism preparedness. Our State strategy is the product of a collaborative, community-based effort. It sets the direction for synchronizing efforts and making wise choices. It also provides a process for collectively planning and coordinating statewide homeland security efforts to include the setting of standards, priorities, and policies. This assures funding is applied against resource gaps that have been identified through objective assessments and are therefore prioritized in the State's action plans. The strategy is a constantly evolving one. We will evaluate our progress, learn, and change as necessary.

We are faced with daunting challenges matched only by the multitude of opportunities to secure our state – our homeland.   The consequences of not being prepared are unacceptable. Through a conscious, calculated and collaborative strategy, we will enhance our preparedness and insure Washington remains a safe and secure place to live, work and raise our families.

The next step in the strategic planning process is to create action plans that develop and prioritize statewide initiatives that will further enhance our ability to prevent, prepare for, respond to and recover from acts of terrorism.



"Ensure a safe and secure Washington for the 21st Century."

APPENDIX A – WASHINGTON STATE HOMELAND SECURITY ORGANIZATIONAL STRUCTURE

The Washington State Homeland Security organizational structure is shown on pages 33 and 34.

Regional Homeland Security Coordination Districts (RHSCD)

(Figure 1)

The Washington State Homeland Security regional planning and coordination structure is divided into nine regions. The regions are made up of one or more counties that include cities, towns, and tribal nations within the regional geographical boundaries. This regional configuration was implemented to distribute federal grant funds, develop emergency responder equipment priority lists, plan and execute training exercises, create regionally based mutual aid plans, and develop volunteer infrastructure to support citizens' involvement in homeland security initiatives. This regional structure has increased communication and collaboration, to include the sharing of best practices and resource coordination. Operations and physical resources are maintained at the local jurisdiction (county, city and tribal) level, and coordination and planning are facilitated at the regional level.

Domestic Security Executive Group (Figure 2)

The Washington State Domestic Security Executive Group is the state government executive level policy and advisory group to advise the Governor on all matters pertaining to state domestic security.

Emergency Management Council (Figure 2)

The Emergency Management Council (EMC) is a statutory body that advises the Governor and the Director of Washington Military Department on all matters pertaining to state and local emergency management. To accomplish this, the Emergency Management Council:

- Assesses hazards, vulnerabilities, threats, and status of local and state preparedness.

- Coordinates and synchronizes state and local emergency management planning and activities to include compliance with state and federal laws.

- Recommends improvements of state and local emergency management.

- Serves as a forum to discuss, monitor, and support the implementation of identified initiatives.

Committee on Terrorism (Figure 2)

The Committee on Terrorism (COT) develops and recommends statewide homeland security strategies to the EMC. The COT provides a statewide forum that fosters dialogue and information sharing between members representing state, emergency management, emergency medical service, fire, law enforcement (Chiefs/Sheriffs), and public health agencies. Advisory members from a variety of sectors and associations participate and are often involved at the sub-committee level. Standing sub-committees exist for equipment, training, information, intelligence, grants and resources, strategy development and an infrastructure working group. This organizational structure facilitates a statewide approach to planning, equipping, training and exercising our capabilities and building capacities.

The Committee on Terrorism objectives are to:

- Develop strategies for preventing, planning and responding to threats and acts of terrorism.
- Identify resource opportunities and recommend appropriate lead agencies or other lead entities for specific grants.
- Identify, develop and recommend standards for equipment and training for statewide interoperability.
- Provide a forum for general coordination and the exchange of information among local, state, and federal entities.
- Recommend policy changes to improve and enhance statewide preparedness.
- Develop opportunities to engage citizens to support local and regional efforts.

To facilitate collaboration and communication for committee operations, the Washington State Emergency Management Division within the Washington Military Department provides limited unfunded support for both the Emergency Management Council and the Committee on Terrorism.

In addition to the above organizational structure, the following two systems are needed capabilities for homeland security in Washington State. With both systems there is a significant funding gap to create and provide long-term capability in Washington State. The action plans will articulate steps, targets and proposed timelines to create these statewide systems.

The State-Wide Integrated Intelligence System

This system consists of two primary components:

1) The Washington State Joint Analytical Center (WAJAC)
2) Regional Intelligence Groups encompassing the entire State of Washington

The statewide goal of the Integrated Intelligence System is to establish a structure to gather, analyze, and report sensitive threat information throughout Washington State. This system will be a true cross-jurisdictional partnership, integrating local, state, and federal law enforcement, as well as first responders, emergency management, and when appropriate the private sector.

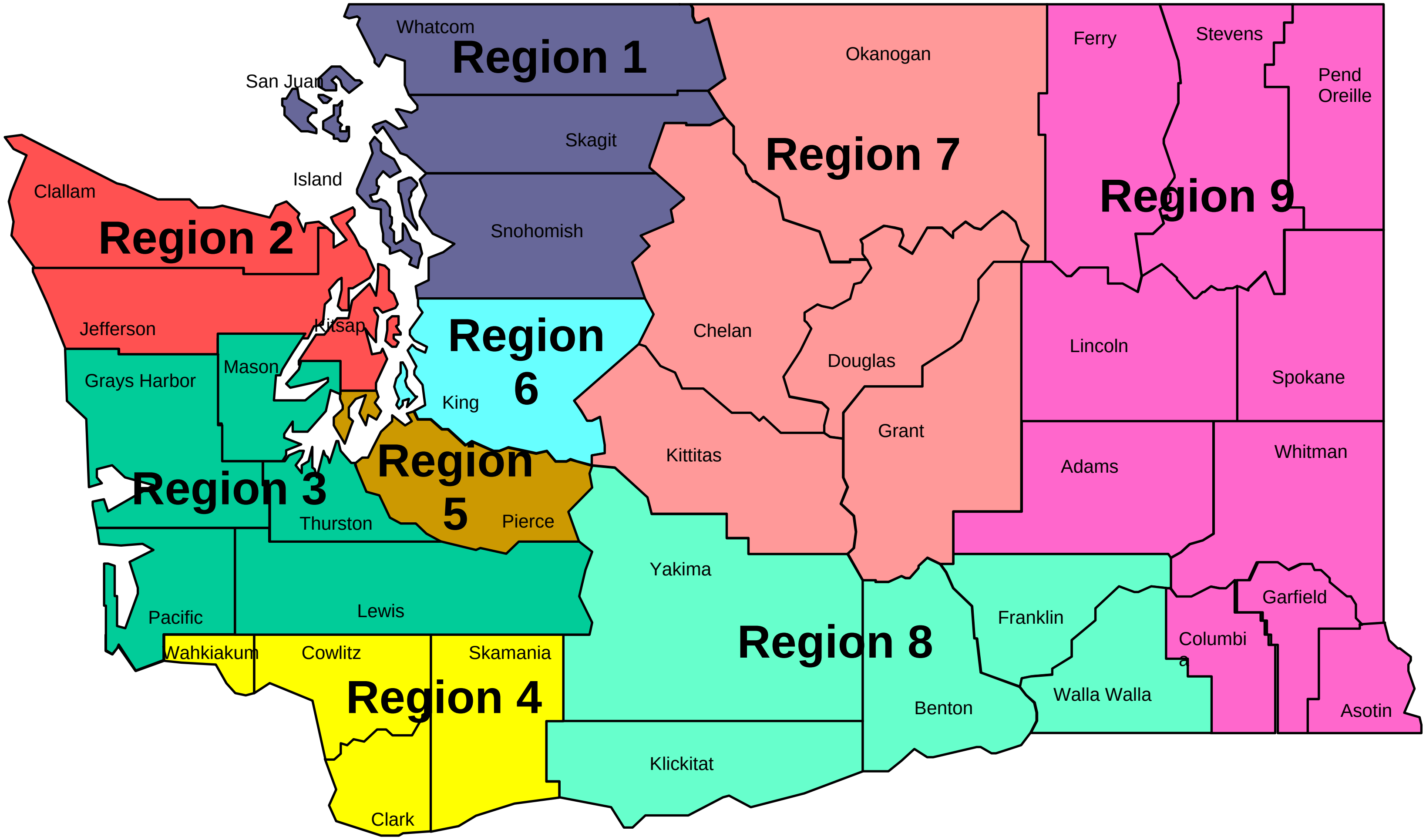
The Homeland Security Institute (HSI)

The statewide training goal for Washington State is to synchronize, customize and standardize training to reach emergency responders in a convenient and efficient manner. The Washington State Homeland Security Institute reflects the ODP blended approach to learning, providing modular training content in a variety of mediums to keep pace with current needs. The Institute will consist of multiple campuses that develop and execute Advanced Distributive Learning Strategies for both resident and distant learning programs. The Homeland Security Institute will consist of virtual campuses of the individual emergency responder disciplines. Each discipline will create an individual virtual campus to partner and train the emergency responder discipline. The mission of the Institute is to train emergency responders to a nationally recognized standard. The Institute, when fully funded, will reach every emergency responder (Law Enforcement, Fire Services, 9-1-1, WA Military Department, Emergency Management, Public Health, Hospital, Public Utilities, Public Ports, DOT, Public Officials and others) through on-line training technologies. There is also the potential with the Institute to increase the educational opportunities for Citizen Corps or other Volunteer organizations.

)

Regional Homeland Security Coordination Districts (RHSCD)

Figure 1

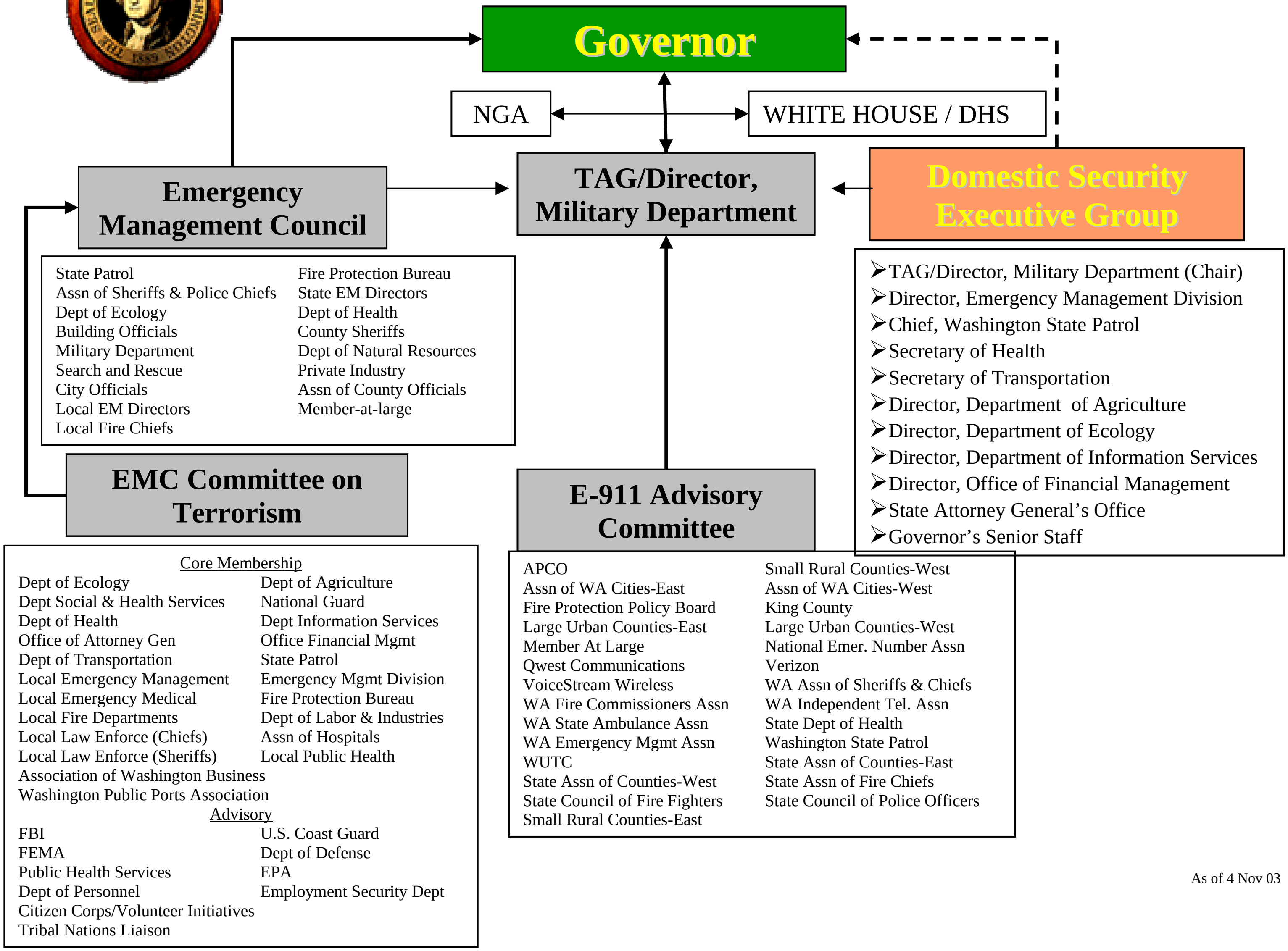


[1] **Note: These coincide with Local Health Regions for Public Health Emergency Planning and Coordination.**

Appendix A – Washington State Homeland Security Organizational Structure

Figure 2

Washington State Domestic Security Infrastructure



Governor

NGA

WHITE HOUSE / DHS

Emergency Management Council

TAG/Director, Military Department

Domestic Security Executive Group

State Patrol
Assn of Sheriffs & Police Chiefs
Dept of Ecology
Building Officials
Military Department
Search and Rescue
City Officials
Local EM Directors
Local Fire Chiefs
Fire Protection Bureau
State EM Directors
Dept of Health
County Sheriffs
Dept of Natural Resources
Private Industry
Assn of County Officials
Member-at-large

- TAG/Director, Military Department (Chair)
- Director, Emergency Management Division
- Chief, Washington State Patrol
- Secretary of Health
- Secretary of Transportation
- Director, Department of Agriculture
- Director, Department of Ecology
- Director, Department of Information Services
- Director, Office of Financial Management
- State Attorney General's Office
- Governor's Senior Staff

EMC Committee on Terrorism

E-911 Advisory Committee

Core Membership

Dept of Ecology
Dept Social & Health Services
Dept of Health
Office of Attorney Gen
Dept of Transportation
Local Emergency Management
Local Emergency Medical
Local Fire Departments
Local Law Enforce (Chiefs)
Local Law Enforce (Sheriffs)
Dept of Agriculture
National Guard
Dept Information Services
Office Financial Mgmt
State Patrol
Emergency Mgmt Division
Fire Protection Bureau
Dept of Labor & Industries
Assn of Hospitals
Local Public Health
Association of Washington Business
Washington Public Ports Association

Advisory

FBI
FEMA
Public Health Services
Dept of Personnel
U.S. Coast Guard
Dept of Defense
EPA
Employment Security Dept
Citizen Corps/Volunteer Initiatives
Tribal Nations Liaison

APCO
Assn of WA Cities-East
Fire Protection Policy Board
Large Urban Counties-East
Member At Large
Qwest Communications
VoiceStream Wireless
WA Fire Commissioners Assn
WA State Ambulance Assn
WA Emergency Mgmt Assn
WUTC
State Assn of Counties-West
State Council of Fire Fighters
Small Rural Counties-East
Small Rural Counties-West
Assn of WA Cities-West
King County
Large Urban Counties-West
National Emer. Number Assn
Verizon
WA Assn of Sheriffs & Chiefs
WA Independent Tel. Assn
State Dept of Health
Washington State Patrol
State Assn of Counties-East
State Assn of Fire Chiefs
State Council of Police Officers

As of 4 Nov 03

APPENDIX B – WASHINGTON STATEWIDE PARTNERS

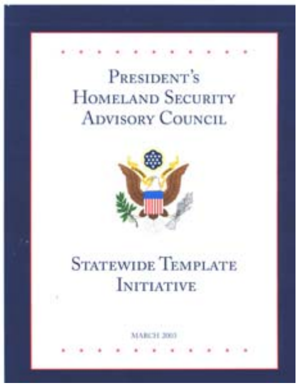
We would like to acknowledge the TEAM WASHINGTON partners for the tremendous statewide input that we received.

- Governor's Domestic Security Executive Group
- Washington State Emergency Management Council
- Committee on Terrorism
- Washington State Emergency Management Division
- Washington National Guard
- U.S. Northern Command
- Washington Military Department
- Regional Homeland Security Coordination Group
- Washington State Emergency Management Association
- Washington Comprehensive Emergency Management Plan (CEMP) Emergency Support Function (ESF) Points of Contact
- Association of Washington Businesses
- Pacific Northwest Economic Region
- American Red Cross
- Native American Tribes
- Governor's Policy Advisor
- Governor's Budget Assistant
- Governor's Office of Indian Affairs
- Federal Emergency Management Agency (FEMA) Region X
- Region 6 Emergency Management Advisory Council
- Pacific Northwest National Laboratory
- Washington Labor Council
- Washington State Cities and Counties
- Washington State Patrol
- Washington State Fire Marshal
- Washington State Department of Health
- Washington State Department of Information Services
- Washington State Office of the Attorney General
- Washington State Department of Transportation
- Washington State Department of Agriculture
- Washington State Office of the Superintendant of Public Instruction
- Washington Citizen Corps/CERT Coordinator

- Washington Commission for National & Community Service/State Citizen Corps Councils
- Washington Public Ports Association
- Washington State Ferries
- Emergency responders (Fire, EMS, Health, Police, Sheriff, E911, Search and Rescue Emergency Managers)
- Washington Association of Sheriffs & Police Chiefs
- Washington State Association of Fire Chiefs
- Washington Association of Hospitals
- Association of Washington Cities
- Association of Washington Counties
- Washington Wing, Civil Air Patrol
- Washington Associations of Contingency Planners
- Washington Public Ports Association
- Washington State Association of Local Public Health Officials
- Washington Poison Center
- Washington EMS and Trauma Care Steering Committee
- Washington Computer Incident Response Center (WACIRC)
- Association of County/City Information Services (ACCIS)
- American Public Works Association
- Washington Voluntary Organizations Active in Disasters
- Washington Water and Sewer Association
- Washington State Water Resources Association

APPENDIX C – Washington State Assessment *(Statewide Template Initiative)*

The Statewide Template Initiative (STI) was developed by the President's Homeland Security Advisory Council. The STI goal is to provide assessment questions for states to provide a foundation for preparing comprehensive and compatible state, local, and tribal Homeland Security plans. The primary objective of the Statewide Template Initiative (STI) is to assist in development of coordinated plans, and it is designed to support implementation of the National Strategy for Homeland Security.


President's Homeland Security Advisory Council

Statewide Template Initiative

March 2003

The statewide template initiative is one of the tools and resources the State of Washington considered to develop the goals and objectives in the Washington Statewide Homeland Security Strategic Plan. At the end of the following (21) STI topic areas is a crosswalk matrix on pages 54-60 that shows the specific relationship between the STI and our strategic goals, objectives, and strategies.

The following input was received from TEAM WASHINGTON partners during the strategic planning process. The bolded questions are from the President's Homeland Security Advisory Council Statewide Template Initiative and Team Washington responses are listed following each question.

The "National Strategy for Homeland Security" defines "State" to be "any state of the United States, The District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, the Canal Zone, the Commonwealth of the Northern Mariana Islands, or the trust territory of the Pacific Islands." The Strategy defines "local government" as "any county, city, village, town, district or other political subdivision of any state, any Native American tribe or authorized tribal organization, or Alaska native village or organization, and includes any rural community or unincorporated town or village or any other public entity for which an application for assistance is made by a state or political subdivision thereof.

Expectations

- ***What does the state expect from the federal government?***

- Collaborative partnership with the states.
- Single point of contact.
- Shared responsibility.
- Clear guidance and expectations.
- Open and proactive communication.
- Systems approach to funding capabilities. The entire spectrum of planning, equipping, training, exercising, sustaining, and replacing should be determined and planned for in increasing our nation's capabilities.
- Timely, accurate, accessible, relevant, useful information and threat intelligence.
- Funding resource support and information.
- Responsiveness to identified needs and initiatives.
- Realistic expectations and timelines.
- No unfunded mandates.
- Streamlined, user friendly processes.
- Leadership.
- Thorough coordination both across the federal government, and also with the states – avoid duplication.
- Wise stewardship of our national scarce resources.
- Education.
- Honesty and Integrity.
- Flexibility, not all states and regions are the same.
- Consistency.

- ❖ Effective structure that makes sense and works well.
- ❖ Do not break existing systems that are effective.

- **What do cities and special purpose districts (e.g., ports) expect from counties and the state government?**

- ❖ In many respects cities and special purpose districts expectations are the same as above:
- ❖ Collaborative statewide partnership of shared responsibility.
- ❖ Incident Management.
- ❖ Single point of contact.
- ❖ Resources – equipment, training, exercises, and staffing.
- ❖ The state of Washington represents their needs to the federal government clearly and consistently.
- ❖ No unfunded mandates.
- ❖ Leverage existing state resources/capabilities to assist and benefit local government.
- ❖ Ability to look globally statewide – no gaps or tunnel vision.
- ❖ Assistance for cities, counties, and regions to plan and coordinate to help meet their goals.
- ❖ Allow cities, counties to execute their own day-to-day operations.
- ❖ Review of local level plans to help ensure accuracy and comprehensiveness.
- ❖ Work to get more realistic deadlines and expectations for grants. The local level has very limited resources.
- ❖ Professional education and exercises for all threat areas.
- ❖ Comprehensive information on what grant opportunities are available to benefit the local level.
- ❖ Flexibility, not all cities, counties and regional coordinating districts are the same.
- ❖ Thorough review and updating of state rules and policy.
- ❖ Support, participation, coordination, leadership, and appropriate funding.
- ❖ Include special purpose districts, such as ports, in all aspects as they are part of the national border, but reside within our state, and are an integral component of the state's overall ability to respond.
- ❖ Clear guidance.
- ❖ Communication – let them know what is happening.
- ❖ Hear and respond to needs and concerns.
- ❖ Timely, accurate, accessible, relevant and useful information.
- ❖ Streamlined, simplified, and user friendly processes.
- ❖ Responsiveness to identified needs.
- ❖ Leadership
- ❖ Honesty and Integrity.
- ❖ Effective structure that makes sense and works well
- ❖ Do not break existing systems that are effective.

- **What should private sector entities expect from federal, state and local governments?**

- ❖ In many respects similar to state and local government expectations. The private sector expects:
- ❖ Be Able to Do Our Job -- Response and recovery that is staffed, trained, equipped, resourced, and ready to respond in the event of a hostile act.
- ❖ Unity of governmental efforts and single point of contact.
- ❖ Optimization of private resources if they must be expended to comply with governmental requirements.
- ❖ Sustained governmental support functions.
- ❖ Contingency plans in place to minimize disruption.
- ❖ Flexible tailored education, assistance, and information – one size does not fit all.
- ❖ Collaborative partnership – open communication and dialogue.
- ❖ Clear guidance and practical leadership.
- ❖ Timely, accurate, accessible, relevant and useful information in particular for the areas of infrastructure protection intelligence.
- ❖ Paying attention to private sector needs and take the appropriate action.
- ❖ Include the private sector in training, equipping plans, and information distribution. Critical infrastructure security is often the first emergency response in case of any attack.
- ❖ Assistance when needed.
- ❖ Education.
- ❖ Competence.
- ❖ Honesty and the "Real Truth" about resources, threats, risks and capabilities.
- ❖ Effective structure that makes sense and works well.
- ❖ Do not break what already works and has proven to be effective.

- **What should citizens expect from federal, state and local governments?**

- ❖ The opportunity to participate and be part of the solution.
- ❖ Do their job well and inexpensively.
- ❖ The answer to, "is everything being done to protect my family?"
- ❖ To know, "how can I help?"
- ❖ Minimal disruption to their lives.
- ❖ Be Prepared and Able to Do Our Job -- Response and recovery that is staffed, trained,

equipped, resourced and ready to respond in the event of a hostile act.
- Effective emergency resource planning and capability.
- Protection from threats – provide them the assurance of security.
- Honesty and the “Real Truth” about resources, threats, risks and capabilities.
- Right to privacy and freedom from intrusiveness.
- Have goals and provide direction.
- A voice in the process and partnership.
- Clear guidance – accurate timely information.
- Training and Education.
- Warning when necessary.
- Assistance during emergencies.
- User friendly, accessible, and timely information and communication.
- Concentrate and do what is important.
- Spend money wisely to add value.
- Ethical management.
- Strong leadership.
- Continuous improvement.
- Competency.
- Listen and hear.
- Response and recovery that is staffed, trained, equipped, resourced, and ready to respond quickly in the event of a hostile act. Thorough planning, training, staffing and equipment – capable of the worst case scenario.
- Proactive communication.
- Standards and assistance tools (checklists, SOPs)
- No barriers between agencies and levels of government – unity of effort.
- Do not break what works well.

- **What should state and local governments expect from their citizens?**

- Be full partners in the effort and commitment.
- Take the time to understand what is going on and how they can help.
- Individual, family and work place preparedness to cope with disruptions until governmental functions can be restored.
- Vigilance.
- Willingness to be educated.
- Assistance when asked = Volunteering.
- Participate in Citizen Corps and Medical Reserve Corps Programs.
- Participate and Volunteer in Police programs.
- Participation in Neighborhood Watch programs.
- Community Emergency Response Team training.
- Responsiveness.
- Cooperation and suggestions (be involved) plus understanding of government’s and private entities role in preventing and responding to emergencies.
- Trust.
- Patience.
- Follow directions in event of a hostile act.
- Reasonable understanding and support.

Continuity of State and Local Government

- **Are plans in place to ensure the timely and successful *“Order of Succession”* of state and local leaders?**

- State of Washington Comprehensive Emergency Management Plan – Section III.A.B.4,5

- Emergency Powers Notebook (April 2003) defines succession, vacancies in offices, Governor’s powers, proclamations, resources in emergencies, state law and procedures, acquisition procedures for emergency resources, contracting procedures, federal and private resources, use of the National Guard, public health emergency information, bioterrorism emergency actions, evacuations, isolation and quarantine rules, and emergency proclamations.

- **What measures exist to ensure the continuity of state and local government ?**

- State of Washington Comprehensive Emergency Management Plan – Appendix 1, Direction and Control. All state agencies, and most local government agencies have developed business continuity plans to use during emergencies. Most have had in place for a long time, were recently revised in some respects for Y2K and are currently being revised in a large number of entities for Homeland Security concerns.

- **Have alternative locations for state and local government operations been identified?**

- Not in all cases, but progress is being made. Federal support for the EOC enhancement funding requested would help improve our capabilities.

- **What collaborative agreements are in place with private industry to ensure business continuity**?
- Most collaborative agreements appear to be between utilities (public and private). Utilities share resources to assist one another during

disaster recovery. There are many other contract type agreements (e.g. fuel in case of emergency) and mutual aid agreements between local governments to provide assistance when local capabilities are exceeded. Business to business entities use contracts to ensure continuity and Washington State has an active association of Contingency Planners. In addition there are many professional organizations and they actively engage with each other to work on partnering to survive disasters.

- **Do state or local mutual assistance compacts address the continuity issue?**

❖ The state and local Comprehensive Emergency Management Plans (CEMPs) address continuity of governments and services. As plans are updated the detail and definition is improving.

Continuity of Critical State Services

- **Have critical state services (e.g., hospitals, emergency medical services, critical infrastructure and associated personnel) been identified?**

❖ Listed in general in the Washington State Comprehensive Emergency Management Plan (CEMP), but not exact personnel.

- **Are contingency plans in place to ensure their reliability, and have they been recently tested?**

❖ Plans are contained in the Washington State Comprehensive Emergency Management Plan (CEMP) under Response Activities. All state agencies, and most local government agencies have developed business continuity plans to use during emergencies. Most have had in place for a long time, were recently revised in some respects for Y2K and are currently being revised in a large number of entities for Homeland Security concerns. They are selectively tested in training exercises – not all have been recently tested.

- **What are your plans to include key representatives of the private sector and those specifically responsible for critical infrastructures in the development of plans supporting the continuity of government, business and critical infrastructures?**

❖ We rely on a system of interaction and liaison with the Committee On Terrorism, the Emergency Management Council, and Private Sector Round Table Discussion.

Critical Infrastructure

- **What are the critical key assets and infrastructures (cyber and physical)?**

The sectors are shown below. We are currently working on a plan and process to define these critical infrastructure specifically in the state.

Agriculture and Food The agriculture and food sector encompasses supply chains for feed, animals and animal products; crop production and the supply chains of seed, fertilizer, and other necessary related materials; post-harvesting components of the food supply chain from processing, production, and packaging through storage and distribution to retail sales, institutional food services, and restaurant or home consumption.

Water The water sector entails fresh water supply and wastewater collection and treatment.

Healthcare and Public Health The healthcare and public health sector includes state and local health departments, hospitals, health clinics, mental health facilities, nursing homes, blood-supply facilities, laboratories, mortuaries, pharmaceutical stockpiles, and veterinary services.

Emergency Services Emergency services consists of 9-1-1, fire, rescue, emergency medical services and law enforcement, and emergency management.

Government Facilities Government facilities encompass military facilities, schools, and government facilities.

Defense Manufacturing Capability The defense industrial base focuses on the capability of industry to produce essential material to support national military objectives; e;g., repair parts, ammunition, chemical defense supplies, MREs, medical supplies.

Information and Telecommunications The information and telecommunications sector In general includes voice and data services.

Energy The energy sector encompasses electricity (dams, power plants, transmission and distribution systems), oil (production, crude oil transport, refining, product transport and distribution, and control and other external support systems) and natural gas (exploration and production, transmission, and local distribution).

Transportation The transportation sector is primarily aviation, maritime, rail, bridges, highways, trucking, busing, pipelines, public ports, mass transit systems.

Banking and Finance The banking and finance sector includes physical structures, financial utilities and human capital; retail and wholesale banking operations, financial markets, regulatory institutions, physical repositories for documents and financial assets.

Chemical Industry and Hazardous Materials The chemical industry and hazardous materials sector contains raw materials, manufacturing plants and processes, distribution and storage systems, research facilities.

Postal and Shipping The postal and shipping sector encompasses key facilities; chain of custody; transportation systems.

Key Assets The key assets sector includes many different aspects to include, but not limited to, historical attractions, monuments, cultural centers, companies of national prominence, commercial centers, stadiums.

- **Who owns them and who is responsible for their operation?**

❖ Approximately 85% is owned by the private sector. We know that the 13 critical industries/systems are owned and operated by hundreds of different companies, public organizations, and even state and local governments. Washington State is working to identify a process and specifics on our infrastructure. A great deal of work remains to be done in this area.

- **Do regionally located critical infrastructures and infrastructure services have the capacity to impact adjacent regions?**

❖ Yes, Washington State borders Canada and other states plus has a significant border on the Pacific Ocean. Critical infrastructure can impact other land and sea regions.

- **Have these infrastructures been identified to all potentially affected regions and Federal Government?**

❖ Not completely. Some of these, like major natural gas pipelines, are known by everyone to have implications for regional impact. Defining all the specifics and identifying them to all affected regions and partners has not been completed.

- **What are the multi-region critical infrastructures single points of failure and interdependencies?**

❖ Fully defining these has not been completed.

- **How are they being addressed?**

❖ Currently we are working to develop the process and policy to identify and address.

- **What measures need to be taken to assure state and local critical infrastructure reliability?**

❖ This depends on the type of the infrastructure and when this is fully developed we can work to better define.

- **Is state and local government partnering with critical private sector industries and infrastructures to help ensure their protection and survivability?**

❖ Not yet, we are working with the Private Sector Roundtables and Private Sector representatives to our committees to establish a methodology, process and working relationship.

- **Has a method been established to allow critical infrastructure owners to query the backgrounds and help ensure the reliability of new employees and periodically those in sensitive positions.**

❖ Private sector and government entities most often have security plans in place to query backgrounds for sensitive positions. A method for ensuring all statewide entities have a system is not in place.

Law

- **Do you have an active system of law reform to identify and address issues related to terrorism?**

❖ Yes; the State Attorney General's Office actively reviewed existing statutes related to terrorism and proposed legislative changes where it thought advisable. In general the State

Attorney General's Office has reviewed state statutes for needed reforms to respond to terrorist threats. The state legislature amended our public records act in light of this review. The State Attorney General's Office worked with law enforcement on amendments to our criminal code but these provisions have been rejected by the state legislature. The State Attorney General's Office has reviewed model statutes with respect to bioterrorism concerns and found no need for changes to our statutes. Similar reviews routinely occurred within the Committee on Terrorism (who meet monthly), a standing committee of our Emergency Management Council that advises the Governor and Adjutant General.

- **Do you have a system for education of individuals affected by legal reforms related to terrorism?**

❖ There is no formal statewide system, but systems are in place that seems to fit this question. For example, when legal changes relating to terrorism have happened in the past involving public records, the Office of the Attorney General authored a white paper covering the new laws and included practice tips. This was provided to all state agencies and local agencies, including emergency management. If the change is in the criminal arena, then dissemination of information would likely happen through the Washington Association of Sheriffs and Police Chiefs as well as through the Washington Association of Prosecuting Attorneys and local law enforcement. The state Committee on Terrorism is often called upon to speak with local agencies on terrorism response issues as well. The Emergency Management Division of the Military Department also has frequent contact with local effected agencies with whom they routinely work.

- **Do you have a plan for continuity of your legal system in the event of a terrorist attack?**

❖ This question has two possible answers. If the question is continuity of the executive branch of government, then yes, there is a plan outlined in both the state constitution and statutes. This has been reduced to writing and the Governor and many members of state government have these laws at their immediate disposal including methods/oaths of "swearing in". While somewhat confidential, protection and movement of the Governor will also be determined in conjunction with the Military Department and the Adjutant General.

❖ If the question focuses directly on the legal system meaning the judicial branch, then no, we do not have a formal plan for the continuity of the legal system. However, there are several parts of the legal system that are used today that answer this question affirmatively. According to our Supreme Court's administrative staff, if there is a vacancy in a judicial position of a court of general jurisdiction, then temporary judges can be appointed or the governor could make a permanent appointment (at least until the next general election). Likewise, the location of a court proceeding can be where the court decides it should be rather than the regular courthouse if it were to be destroyed. This is frequently seen with the Supreme Court where they have heard arguments all over our state or where there is construction, etc. Temporary judges are also commonly seen where a judge in a single judge county is disqualified from a case (there being no other judges within the county to hear the matter). While seldom used, the Chief Justice could appoint a judge in that same situation according to the Supreme Court administrative staff.

Information Sharing and Technology

- **What is the state information-sharing structure?**

❖ Internet, intranet, radio and telecommunications systems makeup the Washington State information-sharing structure.

- **What requirements for specific Homeland Security related information have been provided to local, State, and Federal authorities and the private sector?**

❖ The Washington State Emergency Operations Plan (EOP) provides our all hazard information expectations and response procedures. Specific to an actual incident the state Emergency Operations Center (EOC) will publish supplementary instructions through our WEB EOC capability.

- **What policies and mechanisms (beyond law enforcement) are in place to ensure timely and reliable exchange of intelligence and information among and between local, state,**

and federal authorities and the private sector?

❖ Annex A - Terrorism to the State Comprehensive Emergency Management Plan prescribes the on-scene response organization and procedures, responsibilities through the use of National Interagency Incident Management System (NIIMS) and the Incident Command System (ICS).

❖ ESF 2 to the State Comprehensive Emergency Management provides the telecommunications systems in place to communicate intelligence information to the State Emergency Operations Center.

❖ The State Emergency Operations Center will issue any further event related specifics by WEB EOC to the local jurisdictions on an as necessary basis.

- **What communications limitations currently exist that requires upgrading to take advantage of emerging Homeland Security related information sharing**?

❖ Emerging Homeland Security related information sharing is a vague statement that would need to be better defined to adequately respond.

❖ Without further explanation, the state currently does not have a secure encrypted Internet/Intranet capability that may be necessary for Homeland Security information sharing.

❖ In addition, all state wireless communications are not currently interoperable. We are working towards that and making progress with the creation of standards through the work of the State Interoperability Executive Committee (SIEC), equipment standards defined by the Equipment sub-committee of the state Committee on Terrorism, and funding that becomes available for emergency responder initiatives.

- **Are local, state and federal law enforcement agencies aware of the mechanisms for intelligence sharing that support homeland security efforts (education process)?**

❖ No, this is a continual education process that we are making progress through our statewide coordination by the Washington State Emergency Management Division and our Regional Homeland Security Coordination Districts Council.

- **Do local and state plans provide for outreach to the media before, during, and after terrorist incidents, natural disasters, and all matter of hazards?**

❖ Yes, as prescribed by state and local Comprehensive Management Plans (CEMPs) and Emergency Operation Plans (EOPs).

- **Is there a requirement for secure communications?**

❖ Yes, as defined in ESF 2, State of Washington Comprehensive Management Plan (CEMP).

- **If so, are there assigned/protected frequencies available for use by the emergency response community?**

❖ Yes, as prescribed in Appendix 1, Telecommunications, TAB A to ESF 2, State of Washington Comprehensive Management Plan (CEMP).

- **Has each sector identified and defined the information needed to carry out its homeland security mission?**

❖ In this question and the one below we are not clear on the definition of sector in the context used by the question.

- **Has each sector identified and defined what information needs to be shared among entities within sector and with other sectors?**

❖ No that level of detail has not been defined.

- **Have the differences between the needs of urban and rural responders been identified and accommodated?**

❖ Currently not specifically identified. The State of Washington has a very robust capability to communicate across a wide variety of methods so we do not anticipate that to be a problem, but will work with our regions to better define.

- **What are the plans to continue communication with appropriate private sector and critical infrastructure representatives in the event an emergency precludes normal means of communication?**

❖ Redundant systems that have cross band flexibility, are installed in the Emergency Operations Center capable of communicating by multiple means across any currently known contingency scenario.

Borders

In practice, border security has historically been considered a federal responsibility. Washington State would like to partner with the Bureau of Customs and Border Protection to better define roles and responsibilities and improve the northern border areas security for our state and nation.

Within the Department of Homeland Security the Border and Transportation Security Directorate is responsible for managing the nation's borders and ports-of-entry. The Bureau of Customs and Border Protection within the directorate has developed a National Strategy that uses the Southwest U.S. border as their initial point to strengthen U.S. Borders moving to the coastal borders and then the northern border.

The recently released Border Coordination Initiative (BCI) has eight core initiatives: a) port management, investigations, intelligence, technology, communications, integrity, air/marine, and performance measurement/budget. It consists of a partnership of (14) federal agencies to improve border security initially in the Southwest U.S. border.

The Department of Transportation is responsible for the highways, ferry system and has a vested interest in ensuring the safe/smooth movement of cargo/people on them and across borders. At the point of border security, and operations the responsibility shifts to the federal government.

Within Washington State there are a number of cross border environmental plans, and contact between port authorities that have established planning relationships, but the border security mission has historically been a federal responsibility.

At the state National Guard level we do occasionally provide Counter-drug Aircraft to assist DHS in doing border surveillance according to our law enforcement assistance authority contained in National Guard Regulation 500-2. We have also mobilized soldiers into Title 10 Federal Status to assist with border security. However, in each case, our involvement was limited to providing the personnel and/or equipment for employment by the federal authorities.

Although border security has been traditionally a federal responsibility, the state public facilities ports through newly passed USCG regulations, are required to implement a number of new security responsibilities related to detecting and preventing terrorist acts. It is also important to note that 11 of the state's public ports that receive international vessels over 100 gross tons essentially qualify as border points of entry.

- **Do state and local Border Security plans clearly define the roles and responsibilities of federal, state, and local jurisdictions?**
- **Where do federal and state responsibilities coincide?**
- **Where do federal and state responsibilities diverge?**
- **How are different federal/state roles and responsibilities defined?**
- **Have lines of communication been established with the Department of Homeland Security?**
- **Are procedures in place to track high-risk interstate traffic/cargo?**
- **Are commercial Information Technology reliability standards sufficient to ensure systems?**

Emergency Responders and Emergency Services

- **Who are they?**

Emergency Responders are:
Emergency Level:
Emergency responders, including 9-1-1, fire, law enforcement and emergency medical services personnel, state proprietary or private security personnel who respond to acts or threats of terrorism. They will initiate the ICS system, assess information, take necessary actions, and begin notification of appropriate personnel. They may also likely be exposed to life-threatening hazards.

Second Level: Personnel who respond to incidents of terrorism after the initial response. They may be involved in further development of the ICS system, evacuation, triage, mass care, personnel accountability, identifying and preserving evidence, agent identification, public information, decontamination, and managing site safety. These specialized resources would include Incident Management Teams, Hazardous Materials Teams, emergency medical teams, SWAT Teams, Explosive Teams, and Public Health Response Teams. They may also include other special mobilized resources.

Third Level: Personnel responsible for consequence emergency management activities.

- **What do they require/need?**

❖ Standardized training and specialized equipment as defined by local needs assessment this varies by location. The statewide Committee on Terrorism and Emergency Management Division coordinate and monitor.

- **How are requirements/needs determined and prioritized?**

❖ By state agencies, local level Emergency Management Advisory Councils, Regional Homeland Security Coordinating Districts Council, and the state level Committee on Terrorism/Emergency Management Council.

- **How is consensus gained for requirements/ needs?**

❖ Local council recommendations combined with regional councils and Committee on Terrorism analysis/recommendations submitted to the Emergency Management Council for decision based on consensus for state level decisions.

❖ For regional and local recommendations requirements/needs this is done through their local advisory councils with input/recommendations from the entire emergency responder community.

- **Is there any process to monitor training and equipment acquisition for responders for standardization and quality?**

❖ Yes, the Terrorism programs coordinators for the State of Washington Emergency Management Division and the equipment subcommittee for the statewide Committee on Terrorism (COT) reviews acquisition for standardization and quality.

- **How standardization of equipment purchasing is achieved?**

❖ The statewide equipment subcommittee of the Committee on Terrorism establishes statewide standards. The committee is composed of numerous subject matter experts that are further divided into sub-groups when necessary.

- **How are requirements tied to capability?**

❖ Through local level needs assessments combined with review by the Emergency Management Division and the Committee on Terrorism. The Equipment Sub- Committee examines the level of training, staffing and expertise in the requesting jurisdiction to approve only requirements that match capabilities.

- **How are new capabilities obtained and sustained?**

❖ A systems focus to procurement that considers the full life cycle of equipment to include maintenance, training and exercising. This is analyzed and determined through the Committee on Terrorism. The goal of the COT Equipment Sub-Committee is to support existing capabilities. New equipment for fielding new capability response teams is not approved until we have a core statewide capability in place.

- **Have protected/exclusive communications paths and command authorities been established?**

❖ RCW 70.136.030 designates the Washington State Patrol (WSP) as the Designated Incident Command Agency on all state and interstate highways and in all political subdivisions that did not declare their IC authority or delegated that responsibility to the WSP. A current list of incident command designations is kept at the Mobilization Division of the WSP.

❖ Communication Paths: No answer available yet.

- **Is there a standard, unified, system for incident command?**

❖ NIIMS (National Interagency Incident Management System) Incident Command is in effect, and NIMS established by the NRP will be adopted when finalized.

❖ As specified in Revised Code of Washington (RCW) 38.52.070, 38.52.400, and Washington Administrative Code (WAC) 118-04-180 and WAC 296-824-500010-20.

- **Are the command systems implemented and trained across city, county, and state agencies?**

❖ Yes, as stated above, but not consistently enforced throughout.

- **Have homeland security information require-**

ments been documented?

❖ This is an ongoing process.

- **Are public utility services, public health, hospitals and other medical care providers, and emergency medical service providers involved in planning and training?**

❖ Yes, through the statewide Committee on Terrorism (COT) training subcommittee.

- **Are their emergency plans tested and training evaluated?**

❖ Selectively and in accordance with funding and available resourcing.

National Guard

- **Is the National Guard included in state plans?**

❖ Yes, the Washington State Comprehensive Emergency Management Plan Basic Plan and ESF 20 Military Support to Civil Authorities and Appendix 1- Order of the Governor. The National Guard is also included in many state agency and local jurisdiction plans as well.

- **How many Guardsmen are also emergency responders?**

❖ National Guard records were initially reviewed for Guardsmen who are also emergency responders. This is an on-going process to maintain visibility and assess impacts.

- **Are they included in local and multi-state mutual assistance compacts?**

❖ The procedures for local jurisdictions to obtain National Guard assistance from the state is addressed in the State Comprehensive Emergency Management Plan. They are also found in many state agency and local jurisdiction plans across the state. The procedures for providing interstate National Guard mutual assistance is specifically addressed in the Emergency Management Assistance Compact (EMAC) and while not specifically addressed in the Pacific Northwest Emergency Management Arrangement, is not prohibited.

- **What is the understanding between state and local governments regarding the use of the National Guard to support homeland security operations?**

❖ The procedures for using the National Guard to perform homeland security missions in support of state and local governments are the same as those for performing any Military Support to Civil Authority (MSCA) mission. Those procedures are contained in the Department of Defense Directive 3025.1, Military Support to Civil Authorities; National Guard Regulation 500-1/Air National Guard Instruction 10-8101, Military Support to Civil Authorities; Title 38, Revised Code of Washington; and the State Comprehensive Emergency Management Plan.

❖ The policy, purpose, scope, planning assumptions, concept of operation, organization and procedures are specified in ESF 20 to the State of Washington Comprehensive Emergency Management Plan (CEMP).

- **Are Title 10 and Title 32 US Code authorities and responsibilities clearly understood?**

❖ The authorities, responsibilities and limitations of Title 10 and Title 32 United States Code and Title 38, Revised Code of Washington (for State Active Duty) are well understood and practiced by the National Guard of the State of Washington. While civil authorities are not always aware of the status differences mandated by these laws, the National Guard consults with them and ensures compliance with these laws when National Guard resources are used in civil support missions.

Public Health and Chemical/ Biological/Radiological Terrorism

- **Who is responsible for chemical/biological/ radiological defense efforts?**

❖ State and local health departments share the responsibilities for planning and response to chemical and biological terrorist events. The state DOH retains overall responsibility for a statewide radiological response with added duties to provide local health jurisdictions and other local emergency responders with necessary training in radiological health and safety.

- **Do chemical/biological defense efforts include decontamination of human, livestock, crops, water supplies, and facilities?**

❖ Decontamination efforts include those for humans. Guidance is provided for others.

- **Are agricultural products inspected at the borders and ports?**

❖ Neither state nor local health departments inspect agricultural products at the borders or ports. This is a federal border responsibility.

- **Are there laboratories readily available that can quickly test for agents affecting humans as well as vegetable and livestock diseases?**

❖ The state Public Health Laboratory can quickly test for agents affecting humans and food products. Additional laboratory capacity exists within the Dept of Agriculture and Washington State University to quickly test for plant and animal diseases.

- **Is there a rapid means to communicate critical communicable disease information to appropriate agencies (federal, state and local)?**

❖ The Health Alert Network (HAN) exists that allows rapid communication of critical information among all the public health partners (federal, state, and local).

- **Are chemical/biological/radiological anti-dotes and prophylaxes, antidotes and other emergency pharmaceuticals readily available?**

❖ Yes, they are all available as part of the Strategic National Stockpile (SNS). Readily available is defined as ready within the timelines prescribed in the push packages.

- **Are distribution systems reliable and in place and are they exercised?**

❖ Plans and procedures have been developed and exercised at the federal and state levels. Plans are currently being developed at the local level to accept and distribute the material.

- **Is there a comprehensive public health plan that addresses, federal, state and local resources, legal, economic and operational components?**

❖ No. State, regional and local plans are currently under development.

- **Are hospital and other medical care providers, emergency medical services, and veterinarian and agricultural inspectors included in the plans?**

❖ Regional hospital plans have been developed and will be included in the overall regional public health plans as will those from community clinics and EMS providers. It is not anticipated that veterinarian and agricultural inspectors will be included in the public health plans although there will be a zoonotic disease appendix that will include major responsibilities for veterinarians.

❖ **What methods are used to ensure timely equipment purchasing?**

❖ Ongoing coordination with the regional health departments and the CDC and participation on the Committee on Terrorism equipment subcommittee ensures all equipment purchases are timely and appropriate.

- **Is the public safety community inoculated?**

❖ Large numbers of public health and health care workers have been vaccinated against smallpox. In an emergency these workers will form teams to investigate illness and vaccinate further workers.

- **Have biological, chemical, and nuclear attack exercises been conducted?**

❖ Both chemical and radiological exercises have been conducted at the state level. Health departments are conducting bioterrorism tabletop exercises.

- **How are new capabilities obtained and sustained?**

❖ Currently dedicated federal grant funds are being supplied to state and local health departments from both the Centers for Disease and Control and Prevention (CDC and the Health Services and Resources Administration (HRSA). These funds allow public health capacity building to be sustained.

Private Sector

- **How is the Private Sector being incorporated into your planning process?**

❖ Private sector representatives are included on all statewide major homeland security committees (EMC, COT) and are included in statewide emergency management associations to include the Washington State Emergency Management Association.

❖ The state is also conducting Private Sector roundtable discussions at the CEO level to form a solid partnership between all levels of government and the business community.

- **What public/private sector agreements are in place to ensure effective partnerships between state and local governments and the private sector?**

❖ There are several contingency plan agreements as in the case of utilities for emergency resources.

❖ The state includes the private sector in a large variety of commissions and committees to ensure public/private dialogue and partnership.

- **Have key private sector leaders been identified?**

❖ Yes, in some instances and we are working with the Association of Washington Business, trade associations and the Pacific Northwest Economic Region to better define.

- **Have critical private sector industries been identified in terms of their specialized resource capability or economic value?**

❖ No, not yet. We believe there are significant resources and opportunities available for partnership, and will work to better define.

- **Have private sector resources been identified for potential government use through appropriate agreements and contracts?**

❖ No, not yet.

- **Are small and medium sized enterprises integrated into state and local plans?**

❖ No, not yet.

Volunteer Service

- **Are Private Volunteer Organizations, Nongovernmental Organizations and federally sponsored volunteer programs (e.g., Civil Air Patrol, Red Cross, community and faith based, Americorps, and Senior Corps) included in terrorism strategic and operational plans, such as through state and local Citizen Corps Councils?**

❖ Yes, volunteer organizations are included in the statewide strategic planning process and are in operational plans to include: a) ESF 7 Appendix 1, Undesignated Donated Goods and Services Management Plan, and ESF 7, Appendix 2, Voluntary Agency Resource.

- **Have volunteers with specialized expertise and supplemental equipment (e.g., hi-mobility transportation, communication, etc.) been identified?**

❖ Yes, in many instances to include communications capability through ham radio operators (RACES), volunteer medical (MRC), police capability (VIPS), volunteer firefighters community emergency response (CERT) teams, and Civil Air Patrol with their airborne hyperspectral imaging and aerial radiological monitoring capabilities.

- **Do your state and local communities have Citizen Corps Councils to coordinate citizen participation in homeland security activities (see www.citizenscorps.gov)?**

❖ Yes, the State of Washington has Citizen Corps Councils, and they vary in composition and name dependent on the location. The coordination and assistance for groups is coordinated through the Office of the Governor's – Washington Commission for National and Community Service.

Schools

- **Are homeland security issues factored into public and private school operations?**

❖ The State of Washington is working to include homeland security issues into the overall school safety planning and operations.

❖ In addition to general dialogue state schools are partnered with their local emergency management contacts within their counties for information and warning.

- ❖ The state has established a partnership with the Washington State Association of Sheriffs and Police Chiefs to map all state schools for emergency operations purposes.

- ❖ Expanding on that a consortium was also established to develop a school threat assessment. The threat assessment model will be expanded to include homeland security threat elements.

Citizens with Special Needs

- **How do your plans deal with citizens with special needs?**

- ❖ CEMP, Section V.32, 39, 41.
- ❖ Integrated Fixed Facility Radiological and Chemical Protection Plan, Annex B, Section IV.C.3.
- ❖ Emergency Repatriation Plan, Appendix 12 (Counseling)
- ❖ Emergency Repatriation Plan, Appendix 15, Section IV.D 6-7 (Interpreters and Child Care/Foster Care)

Operations and Information Security

- **What activities is divulging information that could support planning for, conduct of, and enhance the effects of terrorist operations?**

- ❖ Previous to 9/11, governments used websites to provide a vast amount of governmental information to the public.

- ❖ Washington State has revised statute to protect from public disclosure sensitive information related to domestic preparedness for acts of terrorism. RCW 42.17.310 protects those portions of records assembled, prepared, or maintained to prevent, mitigate or respond to criminal terrorist acts, which are acts that significantly disrupt the conduct of government or of the general civilian population of the state or the United States and that manifest an extreme indifference to human life, the public disclosure of which would have a substantial likelihood of threatening public safety, consisting of: a) specific and unique vulnerability assessments or specific and unique response or deployment plans, including compiled underlying data collected in preparation of or essential to the assessments, or to the response or deployment plans; and b) records not subject to public disclosure under federal law that are shared by federal or international agencies, and information prepared from national security briefings provided to state or local government officials related to domestic preparedness for acts of terrorism.

- ❖ Identification of buildings, lay of the land, etc., can aid terrorists in hitting the "correct" target; e.g., labeling a facility as a "data center" or aerial photos of areas that contains sensitive sites.

- ❖ Public access to government buildings has, before 9/11, often been uncontrolled.

- ❖ There is a general effort across the state, both public and private to improve security procedures to prevent inadvertent sharing of information that could benefit potential terrorist actions. With the increased awareness brought about by current events there is interest and learning going on at a variety of levels throughout the state.

- **What is being done to correct the practice(s)?**

- ❖ Governments at all levels routinely reassess their information security procedures.

- ❖ Critical/sensitive facilities are often either not identified or with minimal/nondescript identification.

- ❖ Post 9/11, government building public access is often more controlled

- ❖ Education and assistance to help improve security.

- **What resources are required or are being utilized to help improve state, local and private sector operations and information security procedures?**

- ❖ Implementation of more formal/structured computer incident response processes with various levels of government and vendors that include information sharing and notification protocols.

- ❖ Participation in the Multi-State ISAC for cyber-security and physical security issues.

- ❖ Implementation of the Washington Computer Incident Response Center (WACIRC), a cooperative effort among state agencies to collect, evaluates and disseminates information related to network-based security risks in order to defend the state’s computer systems. WACIRC operates as the focal point for agencies as they communicate information and develop guidelines and best practices related to cyber security.

- **What mechanisms are used to disseminate secured information?**

❖ Secure fax, telephone and videoconferencing capability for emergency communications, and warning from the Washington State Emergency Management Operations Center.

❖ There is no national security classified information disseminated by the Washington State Department of Information Services.

❖ Documents that are sensitive and have an exemption to the state's public disclosure laws are clearly marked to indicate their exemption.

❖ Encryption is used to protect/secure sensitive information (e.g., personal data).

- **What are your priority information systems and how is their performance assured?**

❖ "Standard" systems for most technology driven organizations would be financial systems, telecommunications infrastructure, and operational systems critical to the type of business being conducted/supported.

❖ Implementation of processes to ensure disaster recovery capability and business continuity are key to maintaining operations. These are accomplished through use of data backups and offsite storage of backups, hardening of facilities, increased operational security, equipment redundancy (and/or failover technology) to avoid single points of failure, improved automation to minimize human intervention (so systems can continue to perform under hazardous conditions that could require personnel to leave the area), and participation in multi-agency/organization information sharing

Homeland Security Advisory System (HSAS)

- **Has the HSAS been adopted by the state and/or local governments?**

❖ Yes, the HSAS has been adopted by Washington State government.

- **Has the HSAS been tailored for regional needs?**

❖ Yes, tailored guides have been developed for: a) Businesses, Critical Infrastructure and Key Assets, b) Citizens, Neighborhoods and Families, c) Tribal, County and Local Governments, d) State Government Agencies and Offices of Elected Officials, and e) State Government Executive Summary.

- **Has the HSAS been integrated into the state's** emergency public information plan?

❖ Yes, by the Washington State Emergency Division of the Washington Military Department.

- **Has the media been informed of the basic characteristics of the system?**

❖ Yes, and all guides are available on the State website http://emd.wa.gov/site-general/wahsas/wa-hsas-idx.htm. Whenever there is a change in the advisory system, we employ an integrated approach to media inquiries to inform the public by the Governor and other public safety officials of the state coordinated by the Washington Military Department and primarily the Emergency Management Division public information officer.

❖ **Have you translated the advisory system into actual operational use?**

❖ Yes, the HSAS is fully operational and in use currently.

❖ **Is there a standardized system of tasks for each level?**

❖ Yes, and these are listed in the resource guide we have tailored for our state.

❖ **What can state and local governments do to tailor the HSAS for their policy-makers, emergency planners, emergency responders, and public information officers?**

❖ Talk with them and determine their specific needs first. Involve the different sectors in collaboration during the development process, and tailor the guides to meet their needs.

Public Information and Communications

❖ Washington is a home rule state, enabling local governments to be the emergency responders to an emergency. The state's role is to support and coordinate response activities when the emergency exceeds the capabilities of local jurisdictions. Therefore, the state's Comprehensive Emergency Management Plan is a broad, generic document that does not discuss the details of response operations. This allows for a wide range of approaches, giving the state an opportunity to be flexible in dealing with different organizations and different emergencies. Such issues as coordination of state and local resources and pre-scripted messages are addressed in specific hazard plans, such as the Mt. Rainier Lahar Plan or the State Department of Agriculture's animal disease public information plan.

- **Does the state's emergency public information plan integrate the public information resources of all state and local agencies?**

❖ Following Washington's home rule philosophy of governance, the state's Comprehensive Emergency Management Plan directs local governments to be able to "establish a public information office to provide information and instructions to its citizens before, during, and after an emergency disaster. This office should coordinate its emergency public information actions with the state." The state's plan does not provide a detailed outline of resources that will be utilized for state and local emergency response.

❖ There is, however, a widely shared recognition in the public information community that emergency response resources must be coordinated and shared. The state, for example, is a primary participant in the Regional Public Information Network, a computer website and communications network that includes more than 60 government jurisdictions and agencies in the central Puget Sound Region. The state Emergency Management Division maintains lists of state public information officers and coordinates state public information participation in hazard specific exercises such as the Columbia Generating Station nuclear power plant and the Umatilla Chemical Depot. For state wildfire emergency response, EMD has worked closely with the state Department of Natural Resources and the Washington State Patrol to provide coordinated information that is used by all three agencies in media responses. But all of the protocols and procedures are not part of the state's comprehensive emergency plan.

- **Does the emergency public information plan extend to local authorities?**

❖ The state's Comprehensive Emergency Management Plan, Appendix 2 TAB A, states that "Local jurisdictions are responsible for providing its citizens with information on the incident and what immediate protective actions they should take, such as taking shelter or evacuating." The state plan does not outline the specifics of how the local jurisdiction should inform its citizens about emergencies and the protective action decisions to evacuate or shelter in place.

❖ The state plan also requests local governments to establish a public information office to assist citizens before, during and after an emergency. The plan does not direct how the local jurisdiction should establish its local public information office and program. One county, for example, can assemble as many as 50 to 60 public information officers from its departments to operate a county joint information center. Other counties can mobilize public information staff from other local jurisdictions and operate public phone teams with other agencies and citizen volunteers.

- **Are there agreements between state and local jurisdictions regarding who has the lead for various categories of public information?**

❖ The state's Comprehensive Emergency Management Plan, Appendix 2 TAB A describes state and local responsibilities. The state's Comprehensive Emergency Management Plan directs local jurisdictions to inform their citizens with emergency information and what protective actions individuals should take. Other emergency public information will be prepared and distributed according to specific hazard agreements, such as the joint information center procedures for the Columbia Generating Station nuclear power plant. Other agreements exist for the Mt. Rainier Lahar Plan, the Hanford Site, and the Umatilla Chemical Depot.

- **Is the media being consulted and included in public information planning?**

❖ The media is very important to emergency operations and the planning we do to support operations. We do have regular contact with the media regarding emergency public information. Most recently, Puget Sound media provided extensive feedback about state and local emergency information programs in a facilitated discussion following our experience with the Nisqually Earthquake coverage. These comments were used to revise emergency information procedures. As part of our Emergency Management Division Basic Public Information training, media members discuss problems and issues about working with emergency management agencies. This information is used in formulating public information response plans.

- **Does the emergency public information plan include pre-scripted messages designed for rapid dissemination through the media to inform, reassure, and protect the public?**

❖ Our state emergency public information operational protocols include pre-written fact sheets to help the public in emergency situations. Emergency alert system messages, which are the primary responsibility of local jurisdictions, also are monitored under state public information section procedures to ensure coordination of information.

- **Is there specific emergency information training available for elected and appointed officials?**

❖ The Washington Emergency Management Division offers one public information training unit in the Emergency Management for Executive Officials Course. Some elected and appointed officials also take the three-day Basic Public Information Course (G290) that Washington Emergency Management offers twice each year. Besides training for elected and appointed officials, there is a pressing need to standardize public information training. Currently, both the USDA Forest Service and the Federal Emergency Management Agency have basic public information courses. These should be combined since emergency responders and public information officers are being sent to all hazard incidents. The consolidation will help agencies to work together during incidents and will establish call down lists to improve PIO response and organization for large-scale incidents.

Lexicon

- **Is there an accepted, commonly used and universally understood, language among the multiple disciplines of the State and local and response communities?**

❖ The State Comprehensive Emergency Management Plan, Appendix 4 and the glossary/acronym key to this strategic plan.

- **Is the lexicon consistent with the Emerging National Incident Management System?**

❖ Yes, they are consistent and are living documents that are updated frequently. Once the federal National Incident Management System is finalized the state will update their lexicon as required.

Funding

- **How are local operational needs identified, developed, prioritized, and presented to state authorities?**

❖ Local strategic plans.

❖ State regional homeland security coordination districts communications.

❖ State Committee on Terrorism equipment sub-committee research, communications and meetings.

❖ Existing grant processes.

- **How is bottom-up funding consensus achieved?**

❖ Collaborative statewide partnership to include all components for recommendations and priorities with information/recommendations through the Committee on Terrorism to the state Emergency Management Council for decision.

- **How is the state working with local governments to identify and support local priority needs?**

❖ Partnering together at the state/local level through the regional homeland security districts council.

❖ Further state local/partnering in the Committee on Terrorism and State Emergency Management Council level.

❖ On-site assistance visits by state representatives at the local level.

❖ Creating the Emergency Management Task Force on Local Programs to look at "the state of emergency management" in Washington's counties, cities and tribes. The Task Force is performing a strategic review of the ability of local governments and tribes to provide comprehensive emergency management in Washington State. It is also evaluation how effectively existing laws and regulations meet current emergency management challenges.

- **How is the state ensuring local priorities are met?**

❖ Active listening and partnership.

❖ Initiatives included in the state operating budget.

- State/local level councils (i.e., Regional Homeland Security Coordination District Council, Committee on Terrorism, and the Emergency Management Council.)
- Review of plans to include local strategic level plans.
- Including the local level in the state strategic plan development process.
- Linking grant deliverables to resourcing approval.
- Through the Emergency Management Council's Task Force on Local Programs that is looking at the status and needs of emergency management at the local level in our counties, cities and tribes.

- **How does consensus support budget priorities**?

- They work hand in hand with each other in partnership. We believe in Washington State in a collaborative statewide partnership to build our budget priorities through the strategic planning process where we involve statewide partners throughout the process.

- **Are budget priorities supported by the Governor's Office and State Legislature?**

- Yes, the Governor's Office and the State Legislature are a partner in the process through strategic planning and the state's Priorities of Government process done in conjunction with budget preparation.

- **How are federal funds monitored and distributed to meet operational needs of the state and local jurisdictions?**

- Centralized visibility is maintained through the state Committee on Terrorism and Emergency Management Council. Depending on the source of the federal funds the state agency that has proponency coordinates, monitors and tracks grant funding to meet the needs of state and local jurisdiction.

- **What are the roadblocks to the efficient and timely distribution of Federal resources?**

- Restrictive spending specifics that do not meet local needs and excessive or overly complicated grant instructions can be a roadblock to timely distribution of Federal resources.
- Grant processes should be streamlined, simplified and centralized to the largest extent possible to provide for efficient and timely distribution to the local level.

Training, Exercising and Evaluating

- **Is there an integrated testing/evaluation program?**

- Yes, supported by training needs assessment in 2001 and the state will participate in an EMAP evaluation in Nov. 2003.

- **Are Emergency Management Accreditation Program (EMAP) evaluation standards utilized?**

- Yes, relatively new (EMAP) evaluation standards, the state initiated an action plan in April 2003 and will undergo assessment in Nov. 2003.

- **Are *"lessons-learned"* integrated into new performance standards?**

- Yes, after every event/evaluated exercise there is a hotwash. Lessons learned are used to then update plans and procedures.

- **Have minimum terrorism training, exercise, and evaluation standards been established for state agencies?**

- Not at this point, but can be addressed by the training sub-committee of the committee on terrorism at some future point in time.

- **Are those same standards required at the local level?**

- Washington is a home rule state, based on local independent conduct of government. Standards are locally determined in accordance with local council specifics.

- **How is success determined?**

- Success is determined by achievement of exercise objectives, measuring subsequent performance in actual events, and subsequent use of lessons learned to modify plans and procedures.

- **Will Field Exercises and Tabletop Exercises be a component of the evaluation methodology?**

- Yes, the state of Washington uses Field Exercises and Tabletop Exercises as part of its total exercise/evaluation program.

- **Have state level documents been refined to reflect the changing response requirements of terror related incidents.**

❖ Yes, the terrorism annex to the state Comprehensive Management Plan was published in 2002. In addition the state Emergency Operations Plan was refined to add terrorism specific response procedures. The state also tailored security advisory system guides for respective sectors.

- **Field Operating Guide?**

❖ The state has an Emergency Operations Plan.

- **Operating Procedures?**

❖ Yes, the state of Washington has an Emergency Operations Plan (EOP) that includes terrorism related procedures.

- **Modifications to the state Comprehensive Emergency Management Plan?**

❖ Yes, Terrorism Annex A to the state Comprehensive Emergency Management Plan (CEMP) was published in 2002.

- **Is there a joint training program for responding to acts of terrorism that involve appropriate representatives from critical infrastructures?**

❖ Not as this point, but as our work progresses on critical infrastructure this can be incorporated.

- **Is there a process to review and provide recommendations to corporate security at critical infrastructure sites?**

❖ Not at this point, but the state includes the private sector on all terrorism related committees, and conducts private sector roundtable discussions so this can be incorporated in the future.

- **How is standardization of training/equipment and interoperability both vertically and horizontally assured?**

❖ The sub-committees for Equipment and Training of the Committee on Terrorism work to ensure interoperability and standardization.

- **What training and maintenance programs are in place to sustain new capabilities?**

❖ Primarily locally determined, but we are also working to develop and fund a statewide homeland security training institute.

Planning and Change Management

- **How are strategic processes adapted to changing capabilities and conditions?**

❖ Through periodic review and a collaborative and participative process to make continuous improvement within our total commitment to providing quality government operations.

- **How are plans adapted to sustain new capabilities and ensure long-term success?**

❖ Through periodic review and updating. The Washington State Emergency Management Division provides assistance for plans review and development.

- **How are specific goals identified and measures of performance applied to objectively assess and manage existing efforts and track new initiatives in statewide plans?**

❖ The State of Washington is committed to the strategic planning process and has incorporated it into the planning budgeting cycle and into performance agreements at all levels of state government.

Statewide Template Initiative (STI) Assessment

The statewide template initiative is one of the tools and resources the State of Washington considered to develop the goals and objectives in the Washington Statewide Homeland Security Strategic Plan. The gaps/status of the (21) STI topic areas helped provide focus for strategies in this strategic plan to ensure a safe and secure state for our residents. The crosswalk shows the specific relationship between the STI and our goals.

STI Topic	Assessment and Gaps	Crosswalk to Strategic Plan Themes and Goals
Expectations	• Good awareness of own expectations. • Need to: ☑ Improve understanding of expectations from other viewpoints.	• Partnership and Leadership
Continuity of State and Local Government	• Plans are generally in place. • Need to: ☑ Train and practice continuity of state and local government plans. ☑ Ensure alternate locations for continuity of government are identified and functional. ☑ Expand private industry agreements and plans currently in place for some business areas throughout the business sector. ☑ Improve the detail and definition of mutual aid plans.	• Partnership and Leadership • Emergency Preparedness/Response - Education & Training • Emergency Response & Recovery - Minimize Damage & Recover From Attack
Continuity of Critical State Services	• Plans are generally in place. • Need to: ☑ Improve detail of critical services listings . ☑ Increase connectivity with the private sector by adding representation from key sectors.	• Partnership and Leadership • Emergency Preparedness/Response - Education & Training • Emergency Response & Recovery - Minimize Damage & Recover From Attack
Critical Infrastructure	• Sectors are defined. • Need to: ☑ Develop infrastructure assessment plan and process. ☑ Identify critical infrastructure and ownership for these assets. ☑ Identify infrastructure interdependencies, impacted sectors and regions. ☑ Develop infrastructure protective measures and plans. ☑ Build infrastructure partnerships and relationships.	• Partnership and Leadership • Reduce Vulnerabilities • Emergency Response & Recovery - Minimize Damage & Recover From Attack

STI Topic	***Assessment and Gaps***	***Crosswalk to Strategic Plan Themes and Goals***
	☑ Ensure effective communication systems are in place to communicate threat information, advisories and protective measures within infrastructure networks. ☑ Establish methodology for background checking employees in critical infrastructure positions.	
Law	• Existing laws have been reviewed in general by the Attorney General's Office, continuity of state government procedures are generally in writing, and education systems for legal reforms appear to be in place. • Need to: ☑ Ensure all state agencies have continuity of government and critical services in place, employees are educated and plans are exercised. ☑ Ensure a system is fully in place to monitor state and federal legislation for homeland security impacts. ☑ Develop a formal plan for judicial branch continuity in case of terrorism or other natural disaster.	• Partnership and Leadership • Prevent Attack
Information Sharing and Technology	• The state does have internet, intranet, telecommunications and radio information sharing capability. • Need to: ☑ Define interoperability standards information sharing systems. ☑ Inventory information sharing systems. ☑ Resolve gaps between existing information sharing systems. ☑ Define communications protocols and methodology for statewide connectivity. ☑ Develop information sharing parameters and templates. ☑ Improve the detail for policies and procedures to share information. ☑ Train and exercise statewide information sharing. ☑ Create a detailed, interoperable wireless communication plan. ☑ Provide detailed and ongoing education for local, state, tribal and federal law enforcement agencies on the mechanisms of information sharing. ☑ Include outreach to the media in all plans for relevant information.	• Communication • Prevent Attacks • Emergency Preparedness/Response - Education & Training

STI Topic	***Assessment and Gaps***	***Crosswalk to Strategic Plan Themes and Goals***
	☑ Improve secure communications capability. ☑ Define information requirements for each sector. ☑ Continue our initial efforts to connect with the private sector and establish an emergency and information sharing network.	
Borders	• Historical border responsibilities are understood. • Need to: ☑ Partner with the Bureau of Customs and Border Protection to define roles and responsibilities and work on actions to improve the northern border area security. ☑ State public facilities ports are now implementing a number of new security responsibilities through the newly passed USCG regulations. Need to understand and ensure plans reflect that all 11 public ports that receive vessels over 100 gross tons are now border ports of entry. ☑ Improve understanding of capacity and capability of port and border security efforts.	• Partnership and Leadership • Prevent Attacks • Reduce Vulnerabilities
Emergency Responders and Emergency Services	• Emergency responders and levels were defined by the statewide Committee on Terrorism. • Need to: ☑ Continue to develop and refine standards for equipment and training requirements. ☑ Continue to improve the requirements determination, prioritization, consensus and monitoring process for planning, equipping, training and exercises. ☑ Develop an Incident Management Team capability. ☑ Develop statewide education and training for NIMS and implement NIMS when finalized. ☑ Implement command systems uniformly across all levels of government (city, county, state agencies). ☑ Include all sectors of responders in planning, training, exercises and ensure interoperable equipment for connectivity. ☑ Comprehensively exercise and test emergency plans.	• Partnership and Leadership • Communication • Emergency Preparedness/Response - Education & Training • Emergency Response & Recovery - Minimize Damage & Recover From Attack
National Guard	• The National Guard is included in current state emergency plans. • Need to: ☑ Define who and how many Guardsmen are	• Partnership and Leadership • Emergency Preparedness/Response - Education &

STI Topic	***Assessment and Gaps***	***Crosswalk to Strategic Plan Themes and Goals***
	statewide emergency responders. ☑ Determine the impact of Guardsmen with dual roles as local emergency responders. ☑ Improve the detail and definition of National Guard responsibilities in statewide emergency response plans.	Training • Emergency Response & Recovery - Minimize Damage & Recover From Attack
Public Health and Chemical/Biological/Radiological Terrorism	• State and Local health jurisdictions and hospitals have been engaged in a regional planning process. • Need to: ☑ Ensure urgent disease reporting to local public health 24/7. ☑ Coordinate statewide deployment of the Strategic National Stockpile. ☑ Develop or enhance laboratory public health emergency plans and protocols. ☑ Deliver appropriate public health education and training to emergency response partners. ☑ Integrate hospital laboratories into public health preparedness efforts. ☑ Ensure effective communications connectivity between state and local public health agencies, hospitals, and emergency management agencies. ☑ Conduct public health drills and exercises. ☑ Develop agriculture plans, capacity and capability to protect the state from potential agri-terrorism threats.	• Partnership and Leadership • Emergency Preparedness/Response - Education & Training • Emergency Response & Recovery - Minimize Damage & Recover From Attack
Private Sector	• A dialogue has been established with the private sector. ☑ Partner with the Private Sector to: 1. Facilitate dialogue with the business community through chambers of commerce and trade associations. 2. Create EOC representation to bridge to business during disasters. 3. Link statewide business community to the domestic security infrastructure. 4. Enhance information sharing by creating a business emergency network. ☑ Create educational presentations/materials/templates for businesses. ☑ Explore the best communication means to continue to engage the business community.	• Partnership and Leadership • Emergency Preparedness/Respo - Education & Trainin • Emergency Response & Recovery - Minimize Damage & Recover From Attack
Volunteer Service	• Volunteers are included in the planning process and there are many active citizen groups in the	• Partnership and

STI Topic	***Assessment and Gaps***	***Crosswalk to Strategic Plan Themes and Goals***
	state that are incorporated into emergency planning. • Need to: ☑ Publicize volunteer opportunities throughout the state. ☑ Include volunteers in planning, training, exercises and equipping efforts. ☑ Establish and maintain a database of volunteer resources. ☑ Include volunteers in communication and information systems. ☑ Develop outreach for underserved and under-represented populations. ☑ Create victim assistance programs.	Leadership • Emergency Preparedness/Response - Education & Training • Emergency Response & Recovery - Minimize Damage & Recover From Attack
Schools	• The Washington State legislature has provided funding to digitally map all high school buildings. Mapping will assist emergency responders by providing essential elements of building/campus infrastructure in case of an emergency. Funding was also provided for a school security threat assessment process for each campus. Ultimately both initiatives will assist schools to develop training and drills to enhance safety planning efforts. • All nine Educational Service Districts (ESD's), and three select schools districts, were recently awarded a joint Dept. of Homeland Security/Dept. of Education emergency preparedness and response grant, designed to assist regions to upgrade current plans and safety collaborations. • The Office of Superintendent of Public Instruction (OSPI) and the Washington State Emergency Management Division (EMD) have jointly developed and provided school incident command training to school administrators and safety teams. • Funding has also been provided by the legislature to provide safety and security training to school security, law enforcement and administrators regarding safety planning and emergency response procedures. A school security academy curriculum has been developed in concert with the Washington State Criminal Justice Training Commission, and a training schedule is currently being developed. • School nurses in Washington State will have the opportunity in 2004 to participate in a special disaster preparedness/emergency response training developed through a national grant.	• Partnership and Leadership • Reduce Vulnerabilities • Emergency Preparedness/Response - Education & Training • Emergency Response & Recovery - Minimize Damage & Recover From Attack

STI Topic	***Assessment and Gaps***	***Crosswalk to Strategic Plan Themes and Goals***
	• Need to: ☑ Complete the high school mapping and security assessment process. ☑ Promote emergency response training and drills that include schools and community agencies to refine procedures and update policies. ☑ Develop a regional emergency notification and communication system that focuses on schools. ☑ Coordinate training and drills between the various sponsoring agencies to address the inter-related needs of schools and other entities. ☑ Include schools in community agency-generated disaster preparedness and emergency response trainings and exercises.	
Citizens with Special Needs	Although citizens with special needs are included in current statewide emergency planning this area can be improved. • Need to: ☑ Actively include in homeland security planning, training, and exercising efforts. ☑ Build relationships with the special needs service community.	• Partnership and Leadership • Communications • Emergency Preparedness/Response - Education & Training • Emergency Response & Recovery - Minimize Damage & Recover From Attack
Operations and Information Security	Governments at all levels routinely reassess the information security procedures. WACIRC is operational and serves as a focal point for information and education. • Need to: ☑ Continue cyber security improvements, education and coordination. ☑ Fully establish a homeland security communications plan for both secure and non-secure means to communicate internally and externally to statewide and federal partners. ☑ Develop and implement intelligence information sharing guidelines.	• Communication • Reduce Vulnerabilities • Emergency Response & Recovery - Minimize Damage & Recover From Attack
Homeland Security Advisory System (HSAS)	• The HSAS is implemented within Washington State and tailored educational guides are available. • Need to:	• Communications • Emergency Preparedness

STI Topic	***Assessment and Gaps***	***Crosswalk to Strategic Plan Themes and Goals***
	☑ Continue dialogue with statewide and federal partners to identify system issues, resolve and work to improve the system. ☑ Improve publication of homeland security activities.	
Public Information and Communications	• Well established public information systems are in place for Washington State. • Need to: ☑ Include the media in education, training and exercise opportunities. ☑ Provide terrorism information and educational materials tailored to meet the unique needs of sectors (e.g., citizens, businesses, governments, tribal nations).	• Communications • Emergency Preparedness/Response - Education & Training
Lexicon	• The strategic plan has a current comprehensive homeland security acronym listing and glossary. • Need to: ☑ Continue to maintain glossaries and acronym guides so the state has universally understood language.	• Partnership and Leadership
Funding	• The state has a strategic plan and an effective statewide collaborative process in place. • Need to: ☑ Create a homeland security priority list for funding. ☑ Maintain visibility of homeland security funding. ☑ Identify all available funding opportunities. ☑ Coordinate statewide to avoid duplication of effort and resources. ☑ Streamline processes. ☑ Focus acquisition strategies to achieve core statewide capability and build above that based on specific threats. ☑ Make interoperable procurement decisions.	• Partnership and Leadership • Resource Capacity
Training, Exercising and Evaluating	• Emergency training, exercising and evaluation programs are in place for the state. • Need to: ☑ Develop, plan and exercise for WMD preparedness and certification. ☑ Develop the capability to efficiently and effectively train emergency responders. ☑ Train and implement NIMS when finalized by the federal government.	• Partnership and Leadership • Emergency Preparedness/Response - Education & Training

STI Topic	***Assessment and Gaps***	***Crosswalk to Strategic Plan Themes and Goals***
	☑ Fully develop and implement a statewide terrorism education program with educational materials and public information for all sectors (e.g., businesses, citizens, volunteers, emergency responders, government, tribal nations) ☑ Develop a broad based exercise program to leverage existing resources and systems and includes participation from all sectors. ☑ Ensure elected and appointed officials are trained and aware of their Incident Management and Continuity of Government responsibilities. ☑ Research best practices from other states, document and share own state lessons learned.	
Planning and Change Management	• State and local governments are committed to the principles of quality management and do strategic planning. • Need to: ☑ Develop homeland security action plans.	• Partnership and Leadership

Ceremonial Dance at the Return of the Salmon Powwow – Richland, WA

PROTECTING OUR STATE, OUR CITIZENRY, OUR ECONOMY AND OUR ENVIRONMENT.

THE TEMPLATE SUPPORTS THE NATIONAL HOMELAND SECURITY STRATEGY AND INCLUDES:

- Expectations
- Continuity of State and Local Governments
- Continuity of Critical State Services
- Critical Infrastructure
- Law
- Information Sharing and Technology
- Borders
- Emergency Responders and Emergency Services
- National Guard
- Public Health and Chemical/ Biological/Radiological Terrorism
- Private Sector
- Volunteer Programs & Services
- Schools
- Citizens with Special Needs
- Operations and Information Security
- Homeland Security Advisory System
- Public Information and Communications
- Lexicon
- Funding
- Training, Exercising and Evaluating
- Planning and Change Management

APPENDIX D - GLOSSARY

911 (9-1-1): Used to describe the 911 telephone systems, Public Safety Answering Points and associated radio and data systems used to receive calls for assistance from the public, catalog and triage information, direct responders to emergency locations and provide support to field responders until event closure or until particular functions are assumed by others under ICS.

Adversary: Often used as a term to describe an enemy; the term enemy is reserved to indicate adversaries engaged in lethal operations against US forces.

ADNET: Anti-Drug Network. Data sharing system established in the Defense Appropriations Act of 1990 and run by the U.S. Department of Defense. Uses real-time secure communications, data sharing, and data analysis for counter drug efforts.

Anti-Terrorism: Preventive in nature and it entails using "passive and defensive measures… such as education, foreign liaison training, surveillance, and counter-surveillance, designed to deter terrorist activities." It is an "integrated, comprehensive approach … to counter the terrorist threat. The concept has two phases: proactive and reactive. The proactive phase encompasses the planning, resourcing, preventive measures, preparation, awareness education, and training that take place before a terrorist incident. The reactive phase includes the crisis management actions taken to resolve a terrorist incident." (JCS Pub 1-02)

Area Command (Unified Area Command): Established as necessary to provide command authority and coordination for two or more incidents in close proximity. Area Command works directly with Incident Commanders. Area Command becomes Unified Area Command when incidents are multi-jurisdictional. Area Command may be established at an EOC facility or at some location other than an ICP. (NIMS Coordinating Draft).

Assessment: The evaluation and interpretation of measurements and other information to provide a basis for decision making (NIMS Coordinating Draft).

Assisting Agency: An agency directly contributing tactical or service resources to another agency. (NIMS Coordinating Draft)

Asset: Anything that has value to the organization (ISO I3335-1:1996)

Attack: A discrete malicious action of debilitating intent inflicted by one entity upon another. A threat might attack a critical infrastructure to destroy or incapacitate it.

Awareness: The continual process of collecting, analyzing, and disseminating intelligence, information, and knowledge to allow organizations and individuals to anticipate requirements and to react effectively. (NIMS Coordinating Draft)

Biological Agents: The FBI WMD Incident Contingency Plan defines biological agents as microorganisms or toxins from living organisms that have infectious or noninfectious properties that produce lethal or serious effects in plants and animals.

Bioshield (Project): In his State of the Union Address, President Bush announced Project BioShield - a comprehensive effort to develop and make available modern, effective drugs and vaccines to protect against attack by biological and chemical weapons or other dangerous pathogens. Project BioShield will: Ensure that resources are available to pay for "next-generation" medical countermeasures. Project BioShield will allow the government to buy improved vaccines or drugs for smallpox, anthrax and botulinum toxin. Use of this authority is currently estimated to be $6B over ten years. Funds would also be available to buy countermeasures to protect against other dangerous pathogens, such as Ebola and plague, as soon as scientists verify the safety and effectiveness of these products. Strengthen NIH development capabilities by speeding research and development on medical countermeasures based on the most promising recent scientific discoveries; and gives FDA the ability to make promising treatments quickly available in emergency situations - this tightly controlled new authority can make the newest treatments widely available to patients who need it in a crisis.

Bioterrorism: The intentional use of microorganisms, or toxins, derived from living organisms, to produce death or disease in humans, animals, or plants.

Bioterrorism Response Advisory Committee (BRAC): Committee consisting of the Department of Health partners and stakeholders that advises the Department of Health on the creation of its plan for bioterrorism preparedness and response.

Block Grant: Federal grant funds that are allocated based on a predetermined statutory formula.

Category "A" Diseases/Agents: The possible biological terrorism agents having the greatest potential for adverse public health impact with mass casualties. High-priority agents include organisms that pose a risk to national security because they can be easily disseminated or transmitted from person to person; result in high mortality rates and have the potential for major public health impact; might cause public panic and social disruption; and require special action for public health preparedness. The Category "A" agents are: smallpox, anthrax, plague, botulism, tularemia, and viral hemorrhagic fevers (e.g., Ebola and Lassa viruses)

Category "B" Diseases/Agents: Second highest priority agents include those that are moderately easy to disseminate; result in moderate morbidity rates and low mortality rates; and require specific enhancements of CDC's diagnostic capacity and enhanced disease surveillance. Category B diseases are: Brucellosis, epsilon toxin of *Clostridium perfringens,* food safety threats (e.g., *Salmonella* species, *Escherichia coli* O157:H7, and *Shingella)*, glanders, melioidosis, psittacosis, Q fever, ricin toxin, staphylococcal enterotoxin B, typhys fever, viral encephalitis (e.g., Venezuelan equine encephalitix, eastern and western encephalitis), and water safety threats (e.g., *Vibrio cholerae, Cryptosporidium parvum).*

Category "C" Diseases/Agents: Third highest priority agents include emerging pathogens that could be engineered for mass dissemination in the future because of the availability; ease of production and dissemination; and potential for high morbidity and mortality rates and major health impact. The CDC cites Nipah virus and hantavirus as examples.

C-DAT: Columbia Data Analysis Teams. Pilot project sponsored by the FBI and U.S. Department of Justice. C-DAT will be a complete information sharing and integration initiative, compiling data from all possible law enforcement agencies – local, state, and federal in a tri-state area (Washington, Oregon, and Idaho).

Channel of Communication: The official conduit for information flow and coordination of plans, resources, and activities.

Chemical Agents: The Federal Bureau of Investigation (FBI) Weapons of Mass Destruction (WMD) Incident Contingency Plan defines chemical agents as solids, liquids, or gases that have chemical properties that produce lethal or serious effects in plants and animals.

Choking Agents: Compounds that injure an unprotected person chiefly in the respiratory tract (the nose, throat and particularly the lungs). In extreme cases, membranes swell, lungs become filled with liquid, and death results from lack of oxygen; thus these agents "choke" an unprotected person. Choking agents include phosgene, diphosgene, and chlorine.

Civil Support: Department of Defense support to US civil authorities for domestic emergencies, and for designated law enforcement and other activities. Also called CS. (JCS Pub 1-02)

Command and Control: The exercise of authority and direction by a properly designated commander over assigned or attached forces in the accomplishment of the mission; command and control functions are performed through an arrangement of personnel, equipment, communications, computers, facilities, and procedures employed by a commander in planning, directly coordinating, and controlling forces and operations in the accomplishment of the mission (JCS Pub 1-02).

Communications: A method or means of conveying information of any kind from one person or place to another (JCS Pub 1-02).

Communications Security: The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes cryptosecurity, transmission security, emission security, and physical security of communications security materials and information. (JCS Pub 1-02).

Community Policing: a "philosophy of policing, based on the concept that police officers and private citizens working together in creative ways can help solve contemporary community problems related to crime, fear of crime, social and physical disorder, and neighborhood decay." (Trojanowicz, Robert and Bonnie Bucquerox. (1990)*. Community Policing: A Contemporary Perspective.* Cincinnati: Anderson Publishing Co.

Competitive Grant: One in which eligible applicants are solicited to submit concept papers. At the conclusion of the solicitation period, all received concept papers are assessed and ranked. The highest ranked applicants are then eligible for an award upon their completion of all necessary administrative requirements. Their award amount may be linked to their ranking.

Comprehensive Emergency Management Network (CEMNET): Dedicated 2-way Very High Frequency (VHF) low-band radio system. Provides direction and control capability for state and local jurisdictions for administrative use, and during an emergency or disaster. This is an emergency management net belonging to and managed by the Washington State Military Department, Emergency Management Division.

Computer Emergency Response Team: An organization chartered by an information system owner to coordinate and/or accomplish necessary actions in response to computer emergency incidents that threaten the availability or integrity of its information systems (DoDD 5160.54).

Congregate Care Center: A public or private facility that is pre-designated and managed by the American Red Cross during an emergency, where evacuated or displaced persons are housed an fed.

Consequence Management: Measures to alleviate the damage, loss, hardship or suffering caused by emergencies. It includes measures to restore essential government service, protect public health and safety, and provide emergency relief to affected governments, businesses and individuals. Per HSPD-5 crises management and consequence management are merged to a single integrated function referred to as domestic incident management.

Container Security Initiative (CSI): Designed to help protect the United States and a large portion of the global trading system from terrorists who might use container transport to hide weapons of mass destruction and related materials without disrupting legitimate flow of cargo. There are several CSI ports that are operational: Vancouver, Goteborg, Halifax, Rotterdam, Le Havre, Bremerhaven, Hamburg, Antwerp, Singapore, Yokohama, Hong Kong, Felixstowe, and Montreal. CSI requires bilateral agreements to be created with other governments to target and pre-screen high-risk containers in overseas seaports before they are shipped to the United States. Customs inspectors (pre-screeners) will also be stationed in CSI ports, to work with their overseas counterparts.

Continuity of Government (COG): Planning to ensure the continuity of essential functions in any state security emergency by providing for: succession to office and emergency delegation of authority in accordance with applicable law; safekeeping of essential resources, facilities, and records: and establishment of emergency operating capabilities.

Continuity of Operations: Efforts taken within an entity (i.e., agency, company, association, organization, business) to assure continuance of minimum essential functions across a wide range of potential emergencies, including localized acts of nature, accidents, technological and/or attack-related emergencies.

Counterintelligence: Those activities which are concerned with identifying and counteracting the threat to security posed by hostile services, organizations, or by individuals engaged in espionage, sabotage, subversion, or terrorism (JCS Pub 1-02).

Counter-terrorism: Strategic and tactical measures taken, in a collective effort to prevent acts of terrorism as defined by the U.S. Department of Justice.

Credible Threat: The FBI conducts an interagency threat assessment that indicates that the threat is credible and confirms the involvement of a WMD in the developing terrorist incident.

Crime Prevention Through Environment Design (CPTED): A method of reducing the perception of crime, the opportunity for crime, and crime itself by altering the physical environment. Employs territoriality (creates a sense of ownership), access control (increases the perceived risk of crime to potential offenders by restructuring or denying access to crime targets), and surveillance (keep potential intruders or attackers under threat of observation).

Crisis Management: Measures to resolve a hostile situation investigate and prepare a criminal case for prosecution under Federal Law. Per HSPD-5 crises management and consequence management are merged to a single integrated function referred to as domestic incident management.

Critical Agents: The biological and chemical agents likely to be used in weapons of mass destruction and other bio-terrorist attacks. Current lists may be found on the Centers for Disease Control and Prevention Web site: http://www.bt.cdc.gov/Atent/Agentlist.asp and http://www.bt.cdc.gov/Agent/AgentlistChem.asp.

Critical Information: Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (JCS Pub 1-02).

Critical Infrastructure: Those systems and assets – both physical and cyber- so vital to the States, Localities and the Nation that their incapacity or destruction would have a debilitating impact on national, state and local security, economic security, and/or public health and safety. (National Strategy for Homeland Security, p.ix, USA Patriot Act, and modified to reflect state and local perspective)

Crossband Repeater Interconnect System: Expands the crossband repeater system capability to receive transmissions at any of several frequencies and rebroadcasts audio on one or more other radio systems operating at other frequencies.

Crossband Repeater System: The simplest crossband repeater system is a two-channel crossband repeater. These devises connect two radios operating at different frequencies.

Cyber Infrastructure: Within our critical infrastructure sectors (agriculture and food, water, healthcare and public health, emergency services, government facilities, defense manufacturing capability, information and telecommunications, energy, transportation, banking and finance, chemical and hazardous materials, postal and shipping) those cyber related (continuum of computer networks) IT systems and assets; e.g. interconnected computer networks, automated control systems, information systems, servers, routers switches and fiber optic cables that allows our critical infrastructure systems to function (see critical infrastructure definition and the National Strategy to Secure Cyberspace).

Cyberspace: Describes the world of connected computers and the society that surrounds them.

Cyberterrorism: A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda.

Data: Data is unprocessed, unanalyzed raw observations and facts.

Deconfliction Center: A process designed to prevent, coordinate or preclude duplicate investigations by two separate individuals or agencies is called Case/Subject Deconfliction. Event De-confliction is designed to ensure officer safety by preventing two tactical events happening at the same time and the same location. De-confliction systems are generally computer based, some with GIS mapping capability linked to a database.

Design, Fabrication and Construction Monitoring Programs: Typically, codes and ordinances that provide for review of new construction, conditional rezoning petitions, development plans, and special exception petitions for the purpose of decreasing the opportunity for crime and increasing the perception of safety. (For example see Plaster, Sherry and Stan Carter. (1993) *Planning for Prevention: Sarasota, Florida's Approach to Crime Prevention Through Environmental Design.* Tallahassee: Florida Criminal Justice Executive Institute)

Deterrence: The prevention of action by fear of the consequences. Deterrence is a state of mind brought about by the existence of threat of unacceptable counter action. (JCS Pub 1-02). Deterrence in the homeland security threat spectrum means an enemy does not even try faced with the evidence of planning, preparation, public mobilization, and training capable of stopping their objectives.

Disease Condition Database: Washington State's electronic repository for a wide range of health data including notifiable conditions (in development).

Disaster: As used in this plan, this term is broadly defined to include disasters and emergencies that may be caused by any natural or man-made event. A large emergency event is that one beyond a community's ability to address within its own and mutual aid resources.

Disaster or Emergency Declaration: A declaration by the President which authorizes supplemental Federal assistance under the Stafford Act. The declaration is in response to a Governor's request and may cover a range of response, recovery and mitigation assistance for state and local governments, eligible private non-profit organizations, and individuals.

Disaster Medical Assistance Team(DMAT): A DMAT is a deployable national asset that can provide triage, medical or surgical stabilization, and continued monitoring and care of patients until they can be evacuated to locations where they will receive definitive medical care. Specialty DMATS can also be deployed to address mass burn injuries, pediatric care requirements, chemical injury or contamination, etc. The DMAT program is managed by the Department of Homeland Security in coordination with the Department of Health and Human Services.

Disaster Mortuary Operational Response Team (DMORT): A DMORT is a deployable national asset that can assist local authorities in providing victim identification and mortuary services, including: temporary morgue facilities; victim identification by fingerprint, forensic dental, and/or forensic pathology/anthropology methods; and processing, preparation, and disposition of remains. The DMORT program is managed by the Department of Homeland Security in coordination with the Department of Health and Human Services.

Discretionary Grant: Federal grant funds that are distributed to states, units of local government or private organizations at the discretion of the agency administering the funds. Most discretionary grants are competitive and usually have limited funds available and a large number of potential recipients.

Domestic Terrorism: Domestic terrorism involves groups or individuals whose terrorist activities are directed at elements of our government or population without foreign direction.

Emergency: Any natural or man-caused situation that results in or may result in substantial injury or harm to the population or substantial damage to or loss of property. As more explicitly defined in the Stafford

Act, it is any occasion or instance for which, in the determination of the President, Federal assistance is needed to supplement State and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States. (NIMS Coordinating Draft).

Emergency Management Assistance Compact (EMAC) A legally binding mutual aid agreement and partnership between the States that allows them to assist one another during emergencies and disasters.

Emergency Management: The process by which the state and nation prepares for emergencies and disasters, mitigates their effects, and responds to and recovers from them.

Emergency Operations Center (EOC): The protected site from which civil government officials (city/county and state) exercise direction and control prior to and during an emergency incident.

Emergency Operations Plan (EOP): A planning document that 1) assigns responsibility to organizations and individuals for implementing specific actions at projected times and places in an emergency that exceeds the capability or routine responsibility of any one agency; 2) sets forth lines of authority and organizational relationships, and shows how all actions will be coordinated; 3) identifies personnel, equipment, facilities, supplies, and other resources available for use during response and recovery operations; and 4) identifies steps to address mitigation issues during response and recovery activities.

Emergency Responder:

Emergency Level: Emergency responders, including fire, law enforcement and emergency medical services personnel, state proprietary or private security personnel who respond to acts or threats of terrorism. They will initiate the ICS system, assess information, take necessary actions, and begin notification of appropriate personnel. They may also likely be exposed to life-threatening hazards.

Second Level: Personnel who respond to incidents of terrorism after the initial response. They may be involved in further development of the ICS system, evacuation, triage, mass care, personnel accountability, identifying and preserving evidence, agent identification, public information, decontamination, and managing site safety. These specialized resources would include Hazardous Materials Teams, emergency medical teams, SWAT Teams, Explosive Teams, and Public Health Response Teams. They may also include other special mobilized resources.

Third Level: Personnel responsible for consequence management activities to include emergency management.

Emergency Response Coordinator: Person authorized to direct implementation of an agency's emergency response plan.

Emergency Services: A critical infrastructure characterized by medical, police, fire, and rescue systems and personnel that are called upon when an individual or community is responding to emergencies. These services are typically provided at the local level. In addition, state and federal response plans define emergency support functions to assist in response and recovery.

Emergency Support Function: The functional approach that groups the types of assistance that a state is most likely to need (e.g. mass care, health and medical services) as well as the kinds of federal operations support necessary to sustain state response actions (e.g., transportation, communications). ESFs are expected to support one another in carrying out their respective missions.

Essential Elements of Friendly Information – Key questions likely to be asked by adversary officials and intelligence systems about specific friendly (our) intentions, capabilities, and activities, so they can obtain answers critical to their operational effectiveness. Also called EEFI (JCS Pub 1-02).

Farmgate: The value of production for all agricultural products.

Federal Radiological Emergency Response Plan: The plan that describes the Federal response to the radiological and on-site technical aspects of an emergency in the United States and identifies the lead federal agency for the event. The events include one involving the Nuclear Regulatory Commission or state licensee, the U.S. Department of Energy or the U.S. Department of Defense property, a space launch, occurrence outside the United States but affecting the United States, and one involving radium or accelerator-produced material. Transportation events are included in those involving the U.S. Nuclear Regulatory Commission, state licensee, U.S. Department of Energy, or U.S. Department of Defense.

(FAST) U.S. and Canada Free and Secure Trade: FAST is a harmonized clearance process for shipments of known compliant importers. FAST is for shipments destined to the United States (from Canada or Mexico) using highway mode of transport. For trucks to use FAST lane processing, the Mexican manufacturer must be C-TPAT approved, the U.S. importer (of record) must be C-certified, and the commercial driver must possess a valid FAST Commercial License. The cargo release methods for FAST shipments are the National Customs Automated Prototype (NCAP) and the Pre-Arrival Processing System (PAPS)>

Federal Response Plan (FRP) The plan designed to address the consequences of any disaster or emergency situation in which there is a need for Federal assistance under the authorities of the Stafford Act. Twenty-seven Federal departments and agencies including the American Red Cross are signatories to the plan.

FINCEN: Financial Crimes Enforcement Network. A US Department of Treasury program established in 1990 to implement and oversee policies related to money laundering. FINCEN provides information sharing and strategic analysis of domestic and worldwide money laundering developments, trends, and patterns.

Fire Service (FS): Individuals, who on a full-time, volunteer, or part-time basis provide life safety services including fire suppression, rescue, arson investigation, public education, and prevention.

Focus Areas: Categories of emergency preparedness activities states must address in their Cooperative Agreements for Public Health Preparedness and Response for Bioterrorism. Focus areas cover the following topics:
Focus Area A: Preparedness Planning and Readiness Assessment
Focus Area B: Surveillance and Epidemiology Capacity
Focus Area C: Laboratory Capacity – Biological Agents
Focus Area D: Laboratory Capacity – Chemical Agents
Focus Area E: Health Alert Network (HAN)/Communications and Information Technology
Focus Area F: Communicating Health Risk and Health Information Dissemination
Focus Area G: Education and Training

Force Protection: Force protection is often used in the military sense to mean a security program designed to protect our own service members, civilian employees, family members, facilities, and equipment in all locations and situations. (Joint Tactics, Techniques, and Procedures for Antiterrorism, Joint Pub 3-07.2, 17 March 1998)

Fusion Center: An organized structure to coalesce data and information for the purpose of analyzing, linking and disseminating intelligence. A model process is like to include: extract unstructured data, extract structured data and fuse structured data. Fused data are then analyzed to generate intelligence products and summaries for tactical, operational, and strategic commanders. Types of analysis typically conducted in a fusion center include; association charting, temporal charting, spatial charting, link analysis, financial analysis, content analysis and correlation analysis.

Governmental Administrative: Elected and appointed officials responsible for public administration of community health and welfare during a WMD terrorism incident.

G-Series Nerve Agents: Chemical agents of moderate to high toxicity developed in the 1930s. Examples include tabun (GA), sarin (GB), soman (GD), and GF.

Hazardous Materials Personnel (HZ): Individuals, who on a full-time, volunteer, or part-time basis identify, characterize, provide risk assessment, and mitigate/control the release of a hazardous substance or potentially hazardous substance.

Health Alerts: Urgent messages from the CDC to health officials requiring immediate action or attention. The CDC also issues health advisories containing less urgent information about a specific health incident or response that may or may not require immediate action, and health updates, which do not require action.

Homeland Defense: The protection of US territory, sovereignty, domestic population, and critical infrastructure against external threats and aggression. Also called HLD. See also homeland security and civil support. (JCS approved definition)

Homeland Security: (1) A concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. (National Strategy for Homeland Security p.2)
(2) The preparation for, prevention of, deterrence of, preemption of, defense against, and response to threats and aggressions directed towards US territory, sovereignty, domestic populations, and infrastructure; as well as crisis management, consequence management, and other domestic civil support. Also called HLS. See also homeland defense and civil support (JCS approved definition).

Hospital Emergency Incident Command System(HEICS): HEICS is the Incident Command System (ICS) framework specific to hospitals. The system was developed by the State of California and is used by many hospitals in Washington State. It specifies the chain of command and functional positions that may be required during a hospital's response to an emergency situation.

Hotwash: An after action review for events or training that discusses what went right, what went wrong and what to do differently next time.

Incapacitating Agents: An agent that produces temporary physiological and/or mental effects via action on the central nervous system. Effects may persist for hours or days and victims usually do not require medical treatment; however, such treatment does speed recovery.

Incident Action Plan (IAP): Contains objectives reflecting the overall incident strategy, specific tactical actions and supporting information for the next operational period. The plan may be oral or written. When written, the plan may have a number of forms as attachments (e.g., traffic plan, safety plan, communications plan, and maps). (NIMS Coordinating Draft).

Incident Command System: The Incident Command System (ICS) is the combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in the management of resources at emergency incidents. It is used for all kinds of emergencies, and is applicable to small as well as very large and complex incidents. ICS is used by all levels of government (Local, State, Tribal, and Federal) to organize field level operations. (NIMS Coordinating Draft).

Incident Commander: The person responsible for the overall management of the incident, approval of action plans, and providing direction and control for the command and staff sections of the incident command structure. In a Unified Command structure, the IC collaborates and consults with the chiefs and experts from the other disciplines involved in the response.

Information: Processed fact: reporting with or without analysis. It is often prepared for publication or dissemination in some form and is intended to inform rather than warn or advise.

Information Security: The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. Also called INFOSEC (JCS Pub 1-02).

Information System: The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. Also, Information systems the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate and act on information (JCS Pub 6-0).

Information Warfare: Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks (CJCSI 3210.01).

Infrastructure: The framework of interdependent networks and systems comprising identifiable industries, institution (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of governments at all levels of society as a whole.

Intelligence: The product of adding value to information and data through analysis. Intelligence is created for a purpose. It is the process by which analysis is applied to information and data to inform policy-making, decision-making, including decisions regarding the allocation of resources, strategic decisions, operations and tactical decisions. Intelligence serves many purposes among which are the identification and elimination of threat sources, the investigation and resolution of threats, the identification and treatment of security risk, the elimination of threat sources, the mitigation of harm associated with risk, preemption, response, preparation and operations related to threats and risks.

Intelligence Cycle: The process by which information and data is collected, evaluated, stored, analyzed and then produced or placed in some form for dissemination to the intelligence consumer for use. The cycle consists of: consumer, collector, evaluation, analysis, production, dissemination, consumption, and consumer.

Intelligence Products: The intelligence deliverables. They are the means by which intelligence is communicated to those who will use it. Intelligence products are not limited to written digests or summaries, reports or notes, and can also include oral warnings, alerts, advisories or notices given to the consumer when justified. It also includes oral briefings and other presentations made by the intelligence professional within the scope of his or her duties and responsibilities.

Interagency Incident Management Group (IIMG): The IIMG is made up of senior representatives from Federal departments and agencies, non-governmental organizations, as well as DHS components to facilitate national-level situation awareness, policy coordination, and incident coordination.

International Terrorism: Involves groups or individuals whose terrorist activities are foreign-based and/or directed by countries or groups outside the United States whose activities transcend national boundaries.

Interoperability: The ability of systems or communications to work together.

Joint Field Office (JFO): Federal activities at a local incident site will be integrated during domestic incidents to better facilitate coordination between Federal, state, and local authorities. The JFO is expected to incorporate existing entities such as the Joint Operations Center, the Disaster Field Office and other Federal offices and teams that provide support on scene.

Joint Information Center (JIC): A central point of contact for all news media near the scene of a large-scale disaster. The center is staffed by public information officials who represent all participating federal, state and local agencies to provide information to the media in a coordinated and consistent manner.

Jurisdiction: The range or sphere of authority. Public agencies have jurisdiction at an incident related to their legal responsibilities and authority. Jurisdictional authority at an incident can be political or geographical (e.g., city, county, state or federal boundary lines) or functional (e.g., law enforcement, public health). (NIMS Coordinating Draft).

Laboratory Levels (A,B,C,D): A system for classifying laboratories by their capabilities:
A: Routine clinical testing. Includes independent clinical labs and those at universities and community hospitals.

B: More specialized capabilities. Includes many state and local public health laboratories.
C: More sophisticated public health labs and reference labs such as those run by CDC.
D: Possessing sophisticated containment equipment and expertise to deal with the most dangerous, virulent pathogens and include only CDC and DOD labs, the FBI, and the U.S. Army Medical Research Institute of Infectious Diseases.

Law Enforcement (LE): Individuals, full-time, or on a voluntary basis, who work for agencies at the local, municipal and state levels with responsibility as sworn law enforcement officers.

Local Emergency Planning Committee (LEPC): A term used in the Emergency Planning and Community Right-to-Know Act (EPCRA) (42 U.S.C. 11001: 1986). EPCRA also known as Title II of SARA (Superfund Amendments and Reauthorization Act), was enacted by Congress as the national legislation on community safety. It was designed to help local communities protect public health, safety, and the environment from chemical hazards. To implement EPCRA Congress required each state to appoint a State Emergency Response Commission (SERC) and required each SERC to divide their state into emergency planning districts and to name a local Emergency Planning Committee (LEPC) for each district. Board representation by fire fighters, hazardous materials specialists, health officials, government and media representatives, community groups, industrial facilities, and emergency managers helps ensure that all the necessary perspectives are represented on the LEPC.

Local Government: As defined by the National Strategy for Homeland Security "local government" is "any county, city, village, town, district or other political subdivision of any state, any Native American tribe or authorized tribal organization, or Alaska native village or organization, and includes any rural community or unincorporated town or village or any other public entity for which an application for assistance is made by a state or political sub-division thereof.

Lead Agency: Agency, entity, or combination of, that is recommended by the Committee on Terrorism to the Emergency Management Council to develop a proposal for the use and application of specific grants in support of the state strategic plan on terrorism. They would also manage the grants following guidelines developed and approved by the Emergency Management Council.

Mitigation: Those activities designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident. Mitigation measures may be implemented prior to, during or after an incident. Mitigation measures are often informed by lessons learned from prior incidents. Mitigation involves ongoing actions to reduce exposure to, probability of, or potential loss from hazards. It may include zoning and building codes, floodplain buyouts, and analysis of hazard-related data to determine where it is safe to build or locate temporary facilities. Mitigation can include efforts to educate governments, businesses and the public on measures they can take to reduce loss and injury. (NIMS Coordinating Draft).

National Homeland Security Operations Center (HSOC): The HSOC will serve as the primary national-level hub for operational communications and information pertaining to domestic incident management. Located at DHS headquarters, the HSOC will provide threat monitoring and situational awareness for domestic incident management on a 24/7 basis.

National Interagency Incident Management System (NIIMS): Consists of five major subsystems which collectively provide a total systems approach to all-risk incident management. The subsystems are: the incident command system, training, qualifications and certification, supporting technologies, and publication management.

National Incident Management System (NIMS): A system mandated by HSPD-5 that provides a consistent nationwide approach for Federal, State, Tribal and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. To provide for interoperability and compatibility among Federal, State, and local capabilities, the NIMS include a core set of concepts, principles, and terminology. HSPD-5 identifies these as the incident command system; multiagency coordination systems; unified command; training; identification and management of resources (including systems for classifying types of resources); qualifications and certifications; and the collection, tracking, and reporting of incident information and incident resources. (NIMS Coordinating Draft).

National Security Emergency: Any occurrence, including natural disaster, military attack, technological emergency, or other emergency, that seriously degrades or seriously threatens the national security of the United States (Executive Order 12656).

Need-to-Know: The determination by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. (CIA Directive 1/7. (1998). Security Controls on the Dissemination of Intelligence Information.)

Nerve Agent: Organophosphate ester derivatives of phosphoric acid. Potent inhibitors of the enzyme acetylcholinesterase (AChE), causing a disruption in normal neurologic function. Symptoms appear rapidly with death occurring as rapidly as several minutes. Nerve agents are generally divided into G-series agents and V-series agents. They include tabun (GA), sarin (GB), soman (GD), and VX.

Non-Persistent Agent: An agent that, upon release, loses its ability to cause casualties after 10-15 minutes. It has a high evaporation rate, is lighter than air, and will disperse rapidly. A non-persistent agent is considered to be a short-term hazard; however, in small, unventilated areas, the agent will be more persistent.

Northwest Warning, Alert & Response Network (NWWARN) Is a local and regional information sharing and coordination system pilot project by leveraging present functioning information systems or creating a system where none exists. NWWARN is a network of professionals dedicated to protecting the region’s population and critical infrastructure. The purpose is to provide credible information regarding alerts, threats, and warnings to public and private infrastructure stakeholders, law enforcement and emergency services. NWWARN disseminates and collects information using a broadcast or targeted methodology to include the use of voice, e-mail, mobile text and website updates based on the priority of the message. NWWARN also includes the ability to provide citizens the ability to pass suspicious information tips to the FBI.

Nuclear Weapons: The Effects of Nuclear Weapons (DOE, 1977) defines nuclear weapons as weapons that release nuclear energy in an explosive manner as the result of nuclear chain reactions involving fission and/or fusion of atomic nuclei.

On Scene Commander: A term used to designate the FBI person who provides leadership and direction to the federal crisis management response. The FBI OSC may or may not be the regional Special Agent in Charge (SAC).

Performance Measure: A specific measurable result for each goal that indicates successful achievement.

Physical Infrastructure: Within our critical infrastructure sectors (agriculture and food, water, healthcare and public health, emergency services, government facilities, defense manufacturing capability, information and telecommunications, energy, transportation, banking and finance, chemical and hazardous materials, postal and shipping) those tangible systems and assets; e.g., basic facilities, installations, equipment and personnel needed for a functioning system (see critical infrastructure definition).

Potential Threat Element (PTE): Any group or individual in which there are allegations or information indicating a possibility of the unlawful use of force or violence, specifically the utilization of a WMD, against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of a specific motivation or goal, possibly political or social in nature. This definition provides sufficient predicate for the FBI to initiate an investigation.

Pre-Arrival Processing System (PAPS): A U.S. Customs Automated Commercial System (ACS) border cargo release mechanism that utilizes barcode technology to expedite the release of commercial shipments while processing each shipment through Border Cargo Selectivity (BCS) and the Automated Targeting System (ATS).

Preparedness: The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the capability to protect against, respond to, and recover from domestic incidents. Preparedness is a continuous process. Preparedness involves efforts at all levels of government and within the private sector to identify required resources. Within NIMS, preparedness focuses on establishing guidelines, protocols and standards for planning, training and exercise, personnel qualifications and certification, equipment certification, and publication management. (NIMS Coordinating Draft).

Prevention: Actions to avoid an incident, to intervene to stop an incident from occurring, or to mitigate an incident's effects. Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and as appropriate specific law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity, and apprehending potential perpetrators and bringing them to justice. Prevention also includes measure designed to mitigate damage by reducing or eliminating risks to persons or property or to lessen the potential effects or consequences of an incident. (NIMS Coordinating Draft).

Priority Intelligence Requirements: Those intelligence requirements for which a commander has anticipated and stated priority in the task of planning and decision making. Also called PIRs (JCS Pub 1-02).

Principal Federal Official (PFO): The Secretary may designate a PFO during a domestic incident to serve as the personal representative of DHS locally during an incident. The PFO will oversee and coordinate Federal incident activities and work with local authorities to determine requirements and provide timely Federal assistance.

Private Sector: Organizations and entities that are not part of any governmental structure. It includes for-profit and not-for-profit, and formals and informal structures, including commerce and industry, non-governmental organizations (NGO), and private voluntary organizations (PVO). (NIMS Coordinating Draft)

Public Health Regions: Local health jurisdictions are organized into 9 regions. Each region will develop a plan for resource sharing and coordinated emergency response that will align to the state emergency management plan and will include hospitals, emergency medical services, law enforcement and fire protection districts.

Push Package: A delivery of medical supplies and pharmaceuticals sent from the National Pharmaceutical Stockpile to a state undergoing an emergency within 12 hours of federal approval of a request by the state's Governor

Preparedness: Building the emergency management capability to prepare for, mitigate, respond to, and recover from natural and man-made hazards and terrorist acts through planning, training, education and exercising.

Preempt: Acting emergency to eliminate an opponent's ability to take a specific action. We stop them before they try with our efforts in surveillance, detection, intelligence gathering/sharing, cooperation, early warning and effective command and control.

Prevent: The security procedures undertaken by the public and private sector to discourage terrorist acts. This includes: a) antiterrorism which are defensive measures used to reduce the vulnerability to terrorist acts, to include limited response and containment by local military forces and is also called AT and b) counterterrorism that are offensive measures taken to prevent, deter, and respond to terrorism. (JCS Pub 1-02) Prevention involves the stopping of an enemy before they strike with effective processes, seamless interactive systems, and comprehensive threat, and vulnerability analysis.

Protect: Protection consists of five groups of activities: hardening of positions; protecting personnel; assuming mission oriented protective posture; hardening of positions (infrastructure); protecting people; using physical defense measure; and reacting to an attack. (JCS Pub 1-02) In the event of a strike we successfully defend.

Radiological Dispersal Devices (RDD): A conventional explosive device incorporating radioactive material(s) sometimes referred to as a "dirty bomb."

Rapid Response Information System (RRIS): A system of databases and links to Internet sites providing information to federal, state, and local emergency officials on federal capabilities and assistance available to respond to a consequences of a WMD/terrorism incident. This information is available to designated officials in each state, the ten FEMA regions, and key federal agencies via a protected Internet site and indirectly to the Intranet site through their respective state counterparts. It can be used as a reference guide, training aid, and an overall planning and response resource for WMD/terrorism incidents.

Reasonable Suspicion: When information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. (28 CRF 23.20 (c).

Recovery: The development, coordination, and execution of service- and site-restoration plans; the constitution of government operations and services; individual, private-sector, and public-assistance programs to provide housing and to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration; evaluation of the incident to identify lessons learned; post-incident reporting; and development of initiatives to mitigate the effects of future incidents (NIMS Coordinating Draft).

Red Team: A technique for assessing vulnerability that involves viewing a potential target from the perspective of an attacker to identify its hidden vulnerabilities, and to anticipate possible modes of attack.

Response: Activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans as well as mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into nature and source of the threat; on-going public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice. (NIMS Coordinating Draft).

Risk Management Based Intelligence: An approach to intelligence analysis that has as its object the calculation of the risk attributable to a threat source or acts threatened by a threat source; a means of providing strategic intelligence for planning and policy making especially regarding vulnerabilities and counter-measures designed to prevent criminal acts; a means of providing tactical or operational intelligence in support of operations against a specific threat source, capability or modality; can be quantitative if a proper data base exists to measure likelihood, impact and calculate risk; can be qualitative, subjective and still deliver a reasonably reliable ranking of risk for resource allocation and other decision making in strategic planning and for operations in tactical situations. (David Schwendiman, *Risk Management Model).*

Sentinel Surveillance: Looking at the background level to check for the presence of disease. An example would be when the Department of Health contracts with a farmer to raise chickens then tests the blood of the chickens for the presence of disease.

State: The "National Strategy for Homeland Security" defines "State" to man "any state of the United States, The District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, the Canal Zone, the Commonwealth of the Northern Mariana Islands or the trust territory of the Pacific Islands."

Strategic Goal: Broad statement that describes what we must be able to do to successfully accomplish our mission within each strategic perspective/theme.

Strategic Mission: The tasks assigned to an individual or unit that indicates the actions to be taken. (JCS Pub 1-02) Reflects what we do – the job of homeland security.

Strategic Objective: A specific statement of how a goal will be accomplished.

Strategic Performance Measure/Benchmark: A statement of how attainment of the goal will be measure; the benchmark specifies the criterion for success. What we measure, count and report.

Strategic Planning: The systematic identification of opportunities an threats that lie in the future environment, both external and internal, which, in combination with other relevant data such as threats, vulnerabilities and risks, provides a basis to make better current decisions to pursue opportunities and to avoid threats. It is an orderly process which, sets for basic objectives and goals to be achieved, and strategies to reach those goals and objectives with supporting action plans to make sure that strategies are properly implemented.

Strategic Target: The level we want to achieve within a performance measure/benchmark.

Strategic Theme: Areas we must excel at in order to accomplish our mission.

Strategic Visions: An idealized statement of the best possible future.

Supplanting: Deliberately reducing state or local funds because of the existence of federal funds.

Surge Capacity: Ability of institutions such as clinics, hospitals or public health laboratories to sharply increased demand for their services during an emergency.

Terrorism: Terrorism includes the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. (NIMS Coordinating Draft)

Terrorist Incident: The FBI defines a terrorist incident as a violent act, or an act dangerous to human life, in violation of the criminal laws of the United States or of any State, to intimidate or coerce a government, the civilian population or any segment thereof in furtherance of political or social objectives.

Unified Command: Most often a developing incident crosses jurisdictional boundaries. Unified command allows for each agency to have one incident commander, however, only one will speak at any one time. Depending on the top priorities, the incident commander's "voice" may change frequently. The unified commanders must develop one set of incident objectives, one incident action plan (IAP), and co-locate at one incident.

Unity of Command: The concept by which each person within an organization reports to one and only one designated person. (NIMS Coordinating Draft).

Volunteer: For the purposes of the NIMS, volunteer means any individual accepted to perform services by the lead agency, which has authority to accept volunteer services. (NIMS Coordinating Draft)

Vulnerability: (1) The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. (2) The characteristics of a system that cause it to suffer a definite degradation (incapacity to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. (3) In information operations, a weakness in information systems security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system (JCS Pub 1-02).

Vulnerability Assessment: The Vulnerability Assessment provides a measure to indicate the relative likelihood that a particular facility or incident within the jurisdiction may become the target of a terrorist attack. The factors considered include measures of attractiveness and impact.

Watchout Situations: In fire management and fire service, watchout situations are indicators or trigger points that remind firefighters to reanalyze or to re-evaluate their suppression strategies and tactics. The "watchout situations" in the fire service are more specific and cautionary than the "Ten Standard Fire

Orders." In antiterrorism, the term is used as a metaphor for those observations that can alert trained personnel not just firefighters but law enforcement, public works, private security, or anyone, to be more cautious, more observant, and more likely to report the unusual behavior or activity to the appropriate authorities.

Weapons of Mass Destruction: (A) Any destructive device as defined in section 921 of this title (which reads) any explosive, incendiary or poison gas, bomb, grenade, rocket having a propellant charge of more than four ounces, missile having an explosive or incendiary charge of more than one quarter ounce, mine or device similar to the above,
(B) poison gas,
(C) any weapon involving disease organism, or
(D) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life. (18 U.S.C., Section 2332a)

Zoonotic: Of or relating to zoonosis. An animal disease that can be transmitted to humans, (e.g. ebola, lyme disease, anthrax, rabbit fever, rabies, and swamp fever).

APPENDIX E - ACRONYMNS

AAPA	American Association of Port Authorities
AAR	After Action Report
AASHTO	American Association of State Highway and Transportation Officials
AC	Hydrogen Cyanide (a blood agent)
ACCIS	Association of County/City Information Services
ACOE	Army Corps of Engineers
ACS	Automated Case System (FBI)
ADIS	Arrival Departure Information System
ADNET	Anti-Drug Network
AEL	Authorized Equipment List
AGILE	Advanced Generation of Interoperability for Law Enforcement
AGO	WA State Attorney General’s Office
AIS	Automatic Identification System (Maritime)
ALI	Automatic Location Identification
AMC	Army Material Command (U.S. Army)
AMI	Air and Marine Interdiction Program
AMS	Automated Manifest System
AOR	Area of Responsibility
APCO	Association of Public Safety Communications Officials
APHIS	Animal & Plant Health Inspection Service (DHS)
APHL	Agency for Public Health Laboratories
APIS	Advance Passenger Information System
APTA	American Public Transportation Association
ASCR	Advanced Scientific Computing Research
ASP	Alternative Security Program (Non-SOLAS Vessels)
ASTHO	Association of State and Territorial Health Officials
ARAC	Atmospheric Release Advisory Capability (DOE)
ARC	American Red Cross
ARES	Amateur Radio Emergency Services
ASCR	Advanced Scientific Computing Research
ARG	Accident Response Group (DOE)
ASTHO	Association for State and Territorial Health Officials
ATAC	Anti-Terrorism Advisory Council
ATIX	Anti-Terrorism Information Exchange
ATS	Automated Targeting System
ATSA	Aviation and Transportation Security Act
ATSDR	Agency for Toxic Substances and Disease Registry
ATTF	Anti-Terrorism Task Force
AVIC	Area Veterinary in Charge
AWB	Association of Washington State Business
BATFE	Bureau of Alcohol, Tobacco, Firearms and Explosives
BATS	Bombing and Arson Tracking System (ATF)
BBS	Bureau of Border Security
BCIS	Bureau of Citizenship and Immigration Services
BCRT	Regional Drug Task Force Biological/Chemical Response Team
BCS	Border Cargo Selectivity
BDRP	Biological Defense Research Program (U.S. Navy)
BER	Biological and Environmental Research
BERT	Public Health Bioterrorism Emergency Response Team
BICE	Bureau of Immigration and Customs Enforcement
BOLO	Be On the Lookout
BRAC	Bioterrorism Response Advisory Committee
BRTC	Border Research Technology Center

BSI	Base Support Installation
BSIR	Biannual Strategy Implementation Reports (Grants)
BT	Bioterrorism
BTS	Border & Transportation Security Directorate (DHS)
BW	Biological Warfare
C2	Command and Control
CA	Civil Affairs
CAC	Crisis Action Center
CAEC	County Animal Emergency Coordinator
CAIRA	Chemical Accident/Incident Response and Assistance
CAP	Civil Air Patrol
CAP	Corrective Action Plan
CAPR	Categorical Assistance Progress Reports (Grants)
CARVER	Criticality, Accessibility, Recoverability, Vulnerability, Effect, Recognizability
CAW	Center for Asymmetric Warfare
CBO	Community Based Organizations
CBP	Customs Border Protection
CBS	Customer and Border Protection (part of DHS)
CCP	Citizen Corps Program
CCRF	Commissioned Corps Readiness Force (PHS)
CD	Communicable Disease
CDC	Centers for Disease Control and Prevention
CDRG	Catastrophic Disaster Response Group
CBIRF	Chemical and Biological Incident Response Force (U.S. Marine Corps)
C/B-RRT	Chemical Biological Rapid Response Team (U.S. Army)
CBDCOM	Chemical Biological, Defense Command (U.S. Army)
CBPMO	Customs and Border Patrol Modernization Office
CBRED	Chemical, Biological, Radiological, Environmental Defense Response (U.S. Navy)
CBRNE	Chemical, Biological, Radiological, Nuclear, Explosive
CDAT	Columbia Data Analysis Team
CDP	Center for Domestic Preparedness
CEMNET	Comprehensive Emergency Management Network
CEMP	Comprehensive Emergency Management Plan
CERCLA	Comprehensive Environmental Response, Compensation and Liability Act
CERT	Community Emergency Response Teams
CFDA	Catalog of Federal Domestic Assistance
CFR	Code of Federal Regulation
CG	Phosgene (a choking agent)
CHER-CAP	Comprehensive HAZMAT Emergency Response – Capability Assessment Program
CHIP	Computer Hacking and Intelligence Property
CIAO	Critical Infrastructure Assurance Office
CIP	Critical Infrastructure Protection
CIRC	Computer Incident Response Center
CIRG	Critical Incident Response Group
CIS	Citizenship and Immigration Services
CISM	Critical Incident Stress Management
CIVA	Critical Infrastructure Vulnerability Assessment
CK	Cyanogen Chloride (a blood agent)
CLASS	Consular Lookout and Support System
CLOREP	Chlorine Emergency Plan
COA	Course of Action
COG	Continuity of Government
COPS	Community Oriented Policing Services
COT	Washington State Emergency Management Council Committee on Terrorism
COOP	Continuity of Operations
CMT	Crisis Management Team
CPTED	Crime Prevention Through Environmental Design
CPX	Command Post Exercise
CRRA	Capabilities Review and Risk Assessment

CS	Civil Support
CSEPP	Chemical Stockpile Emergency Preparedness Program
CSA	Customs Self-Assessment
CSI	Container Security Initiative
CSID	Centralized Scheduling and Information Desk (ODP Desk for Reports)
CSG	Council of State Governments
CST	Civil Support Team
CSTARC	Cyber Security Tracking Analysis and Response Center
CSTE	Council of State and Territorial Epidemiologists
CT	Counter-Terrorism
CTAC	Counter-Drug Technology Assessment Center
CTC	Counter-Terrorism Center
C-TPAT	Customs-Trade Partnership Against Terrorism
CX	Phosgene Oxime (a blister agent)
DAE	Disaster Assistance Employee (also called SAE for Stafford Act Employee)
DCD	Disease Conditions Database
DCE	Defense Coordinating Element
DCO	Defense Coordinating Officer
DDO	Deputy Director for Operations
DEA	Drug Enforcement Administration
DEST	Domestic Emergency Support Team
DFO	Disaster Field Office
DHS	U.S. Department of Homeland Security
DHHS	U.S. Department of Health and Human Services
DHSHQ	DHS Headquarters
DIS	Washington State Department of Information Services
DIST	Disaster Information Systems Clearinghouse
DMAT	Disaster Medical Assistance Team (FEMA)
DMORT	Disaster Mortuary Operational Response Team (FEMA)
DNR	Washington State Department of Natural Resources
DPETAP	Domestic Preparedness Equipment Technical Assistance Program
DSHS	Washington State Department of Social and Health Services
DOC	U.S. Department of Commerce
DOD	U.S. Department of Defense
DOE	U.S. Department of Energy
DOI	U.S. Department of the Interior
DOJ	U.S. Department of Justice
DOS	U.S. Department of State (US)
DOT	U.S. Department of Transportation
DRC	Disaster Recovery Center
DRM	Disaster Recovery Manager
DSEG	Governor’s Domestic Security Executive Group
DT	Domestic Terrorism
DUNS	Data Universal Numbering System (Grants)
DWI	Disaster Welfare Inquiry
EAO	Energy Assurance Office
EAS	Emergency Alert System
EC	Emergency Coordinator
EDI	Electronic Data Interchange
EEI	Essential Elements of Information
EFSEC	Energy Facility Site Evaluation Council
EFR	Emergency Responder
EHP	Environmental Health Program, Health Department
EICC	Emergency Information and Coordination Center (FEMA)
EIS	Epidemic Intelligence Service
EMA	Emergency Management Agency (local)
EMC	Washington Emergency Management Council
EMD	Washington State Emergency Management Division
EMAC	Emergency Management Assistance Compact

EMRT	Emergency Medical Response Team
EMS	Emergency Medical Services
EO	Executive Order
EOC	Emergency Operations Center (EOC)
EOD	Explosive Ordnance Disposal
EOF	Emergency Operations Facility
EOP	Emergency Operations Plan or Procedures (EOP)
EPA	U.S. Environmental Protection Agency
EPCRA	Emergency Planning Community Right-to-Know Act
EPLO	Emergency Preparedness Liaison Officer
EP&R	Emergency Preparedness and Response (DHS)
EPZ	Emergency Planning Zone
ERAMS	Environmental Radiation Ambient Monitoring System (EPA)
ERC	Emergency Response Coordinator
ERDO	Emergency Response Duty Officer
ERT	Emergency Response Team
ERT	Environmental Response Team (EPA)
ERT	Evidence Response Team (FBI)
ESA	Energy Security and Assurance
ESA	Environmentally Sensitive Area
ETC	Emergency Telecommunications
ESD	Educational Service Districts
ESF	Emergency Support Function (ESF)
EST	Emergency Support Team (FEMA)
ESSENCE	Electronic Surveillance System for the Early Notification of Community-based Epidemics
FAA	Federal Aviation Administration
FAMS	Federal Air Marshall Service
FAR	Federal Acquisition Regulations
FAS	Federation of American Scientists
FAST CORRIDOR -	Freight Action Strategy for the Everett-Seattle-Tacoma Corridor
FBI	Federal Bureau of Investigation
FCO	Federal Coordinating Officer
FDA	U.S. Food and Drug Administration
FedCIRC	Federal Computer Incident Response Center
FEMA	Federal Emergency Management Agency
FERC	FEMA Emergency Response Capability
FESC	Federal Emergency Support Coordinator
FHWA	Federal Highway Administration
FID	Flame Ionization Detector
FINCEN	Financial Crimes Enforcement Network
FIRECOM	Fire Communications
FLETC	Federal Law Enforcement Training Center
FMAC	Freight Mobility Advisory Committee
FMSIB	Freight Mobility Strategic Investment Board
FOA	Field Operating Agency
FOC	FEMA Operations Center
FOIA	Freedom of Information Act
FPF	Fallout Protective Factor
FRA	Federal Railroad Association
FRP	Federal Response Plan
FRERP	Federal Radiological Emergency Response Plan
FRMAC	Federal Radiological Monitoring and Assessment Center
FPS	Federal Protective Service
FS	Fire Service
FSR	Financial Status Report (Grants)
FSS	Federal Supply Service
FTA	Federal Transit Administration
FTTTF	Foreign Terrorist Tracking Task Force
FTS	Federal Telecommunications System

GA	Governmental Administrative
GA	Tabun (a nerve agent)
GAN	Grant Adjustment Notice
GB	Sarin (a nerve agent)
GCJIN	Global Criminal Justice Information Network
GC/MS	Gas Chromatograph/Mass Spectrometer
GD	Soman (a nerve agent)
GETS	Government Emergency Telecommunications Service
GIS	Geographic Information Systems
GPS	Global Positioning System
GTIN	Global Trade Identification Number
H	Impure Sulfur Mustard (a blister agent)
HACCP	Hazard Analysis and Critical Control Point
HAZCAT	Hazard Categorizing
HAZMAT	Hazardous Material
HAN	Health Alert Network
HAN LAP	Health Alert Network Local Health Assistance Project
HC	Health Care
HD	Homeland Defense
HD	Distilled Sulfur Mustard (a blister agent)
HDER	Homeland Defense Equipment Reuse Program
HEAR	Hospital Emergency Administrative Radio
HEICS	Hospital Emergency Incident Command System
HEPA	High Efficiency Particulate Air
HIDTA	High Intensity Drug Trafficking Area
HIFCA	High Intensity Financial Crime Area
HIVA	Hazard Identification and Vulnerability Assessment
HHS	Health and Human Services
HLS	Homeland Security
HLT	Hurricane Liaison Team (FEMA)
HLW	High Level Waste
HMRU	Hazardous Materials Response Unit (FBI)
HN	Nitrogen Mustard (a blister agent)
HP	Health Physicist
HRSA	Health Resources and Services Administration
HSAS	Homeland Security Advisory System
HSARPA	Homeland Security Advanced Research Projects Agency
HSC	Homeland Security Council
HSEEP	Homeland Security Exercise and Evaluation Program
HIS	Washington State Homeland Security Institute
HSPD	Homeland Security Presidential Directive
HSOC	Homeland Security Operations Center
HZ	Hazardous Materials Personnel
HazMat	Hazardous Materials
IA	Information Analysis
IAEA	International Atomic Energy Agency
IACP	International Association of Chiefs of Police
IAFC	International Association of Fire Chiefs
IAFIS	Integrated Automated Fingerprint Identification System
IAIP	DHS Information Analysis and Infrastructure Protection Directorate
IALEIA	International Association of Law Enforcement Intelligence Analysts
IAP	Incident Action Plan
IC	Incident Command
ICAP	Incident Communications Action Plan
ICDDC	Interstate Civil Defense and Disaster Compact
ICE	Immigration and Customs Enforcement
ICP	Incident Command Post
ICRI	Incident Commander’s Radio Interface
ICS	Incident Command System

IDD	Industrial Development District
IDENT	Automated Biometric Identification System (INS)
IED	Improvised Explosive Device
IGA	Intergovernmental Agreement
IGN	Intergovernmental Network
IIMG	Interagency Incident Management Group
IIPO	Information Integration Program Office
IIT	Nuclear Regulatory Commission’s Incident Investigation Team
IMPC	International Materials Protection & Cooperation
IMS	Incident Management System
IMSA	International Municipal Signal Association, Inc.
IMT	Incident Management Team
INRP	Initial National Response Plan
INS	Immigration and Naturalization Service
INSPASS	INS Passenger Accelerated Service System
IO	Information Operations
IOF	Interim Operating Facility
IP	Improvement Plan
IPFO	Interim Principle Federal Official
IR	Incident Response
IRIS	Incident Response Information System
IS	Information Superiority
ISA	Importer Self Assessment
ISAC	Information Sharing Analysis Centers
ISO	International Standards Organization
ISPS	International Ship and Port Facility Security Code
IST	Incident Support Team
IT	International Terrorism
ITI	International-to-International Transit Program
ITDS	International Trade Data System
ITS	Institute for Telecommunications Sciences
IW	Information Warfare
IWG	Infrastructure Working Group
IWN	Integrated Wireless Network
JCN	Justice Consolidated Network
JFO	Joint Field Office
JIC	Joint Information Center (JIC)
JIS	Joint Information System
JOC	Joint Operations Center
JPA	Joint Powers Authority
JRIES	Joint Regional Information Exchange System
JTF	Joint Task Force
JTTF	Joint Terrorism Task Force
JTWG	Joint Terrorism Working Group
JWICS	Joint World-wide Intelligence Communication System (JWICS)
LCAT	Logistics Closeout Assistance Teams
L	Lewisite (a blister agent)
LE	Law Enforcement
LEA	Law Enforcement Agency
LEIU	Law Enforcement Intelligence Unite
LEO	Law Enforcement Online
LEPC	Local Emergency Planning Committee
LERC	Local Emergency Response Coordinator
LERN	Law Enforcement Radio Network
LETPP	Law Enforcement Terrorism Prevention Program
LFA	Lead Federal Agency
LHJ	Local Health Jurisdictions
LIMS	Laboratory Information Management System
LLEA	Lead Law Enforcement Agency

L-LERC	Local Lead Emergency Response Coordinator
LLW	Low Level Waste
LNO	Liaison Officer
LOCES	Letter of Credit Electronic Certification System
LPHA	Local Public Health Agency
LPHS	Local Public Health System
LRN	Laboratory Response Network
M & A	Management and Administrative Costs (Grants)
MARIP	Multiple Agency Radio Interoperability Program
MCBAT	Medical Chemical and Biological Advisory Teams (U.S. Army)
MEDNET	Medical Emergency Delivery Network
MILES	Miles Integrated Laser Engagement System
MLAT	Mutual Legal Assistance Treaty
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MMRS	Metropolitan Medical Response System
MRC	Medical Reserve Corps
MRTE	Medical Readiness, Training and Education Committee
MTCR	Missile Technology Control Regime
MTSA	Maritime Transportation Security Act
MSA	Metropolitan Statistical Area
MSCA	Military Support to Civil Authorities
NABC	National Agricultural Biosecurity Center
NAC	Nebraska Avenue Complex
NACCHO	National Association for County and City Health Officials
NAED	National Academy of Emergency Dispatch
NAWAS	National Warning System
NCAP	National Customs Automation Program
NCC	National Coordinating Center
NCIC	National Crime Information Center
NCID	National Center for Infectious Disease
NCHRP	National Cooperative Highway Research Program
NCP	National Oil and Hazardous Substances Pollution Contingency Plan
NCPHP	Northwest Center for Public Health Preparedness
NERRTC	National Emergency Response and Rescue Training Center
NCJRS	National Criminal Justice Reference Service
NCP	National Contingency Plan
NCPHP	Northwest Center for Public Health Preparedness
NCR	National Capitol Region
NCRP	National Council on Radiation Protection and Measurements
NCS	National Communications System
NCSD	National Cyber Security Division
NCSL	National Conference of State Legislatures
NDMOC	National Disaster Medical Operations Center
NDMS	National Disaster Medical System
NEDSS	National Electronic Disease Surveillance System
NEIS	National Earthquake Information Service
NENA	National Emergency Number Association
NEMA	National Emergency Managers Association
NERP	National Emergency Repatriation Plan
NEST	National Emergency Search Team (DOE)
NFDA	National Funeral Directors Association
NFPA	National Fire Protection Association
NGB	National Guard Bureau
NGO	Non-Governmental Organization
NIBRS	National Incident-Based Reporting System
NIC	National Incident Commander
NICC	National Interagency Coordination Center
NICS	National Instant Criminal Background Check System

NIFCC	National Interagency Fire Coordination Center
NIH	National Institute of Health
NIMS	National Incident Management System
NIIMS	National Interagency Incident Management System
NIIS	Non-Immigrant Information System
NIIT	Non-Intrusive Inspection Technology
NIOSH	National Institute for Occupational Safety & Health
NIPC	National Infrastructure Protection Center
NIRT	Nuclear Incident Response Team
NISA	National Infrastructure Simulation & Analysis
NIST	National Institute of Standards & Technology
NLECTC	National Law Enforcement and Corrections Technology Centers
NLETS	National Law Enforcement Telecommunications System
NMRT	National NBC Medical Response Team (HHS)
NOAA	National Oceanic and Atmospheric Administration
NODP	National Office of Domestic Preparedness
NPS	National Pharmaceutical Stockpile
NRC	Nuclear Regulatory Commission
NRDA	National Resource Damage Assessment
NRP	National Response Plan
NRS	National Response System
NSC	National Security Council
NSDI	National Spatial Data Infrastructure
NSEERS	National Security Entry-Exit Registration System
NSEP	National Security Emergency Preparedness
NSF	National Strike Force
NSFCC	National Strike Force Coordination Center
NSRP	National Search and Rescue Plan
NSSE	National Security Special Event
NSTS	National Secure Telecommunications System
NTAC	United States Secret Service National Threat Assessment Center
NTIA	National Telecommunications and Information Administration
NTSB	National Transportation Safety Board
NVOAD	National Voluntary Organizations Active in Disasters
NVOCC	Non Vessel Common Carrier
NVRD	Non-Proliferation and Verification R&D
NW WARN	Northwest Warning, Alert and Response Network
ODP	Office of Domestic Preparedness
OEP	Office of Emergency Preparedness
OER	Office of Emergency Response (DHHS)
OES	Office of Emergency Services
OGC	Office of General Counsel
OHS	Office of Homeland Security
OIA	Office of International Affairs
OJP	Office of Justice Programs
OLA	Office of Legislative Affairs
OMB	Office of Management and Budget
ONCRC	Office of National Capital Region Coordination ,
OPHP	Office of Public Health Preparedness (DHHS)
OPSC	Office of Private Sector Coordination
OPSEC	Operational Security
OSC	On Scene Coordinator/Commander
OSC	Operation Safe Commerce
OSLGC	Office of State and Local Government Coordination
PAD	Protective Action Decision
PADO	Public Affairs Duty Office
PAG	Protective Action Guide
PAPR	Powered Air Purifying Respirator
PAPRS	Phone Activated Paperless Request System

PAPS	Pre-Arrival Processing System
PAR	Protective Action Recommendation
PASS	Personal Alert Safety System
PCAPA	Pacific Coast Association of Port Authorities
PDA	Preliminary Damage Assessment
PDD	Presidential Decision Directive
PFA	Primary Federal Agency
PFO	Principal Federal Official
PHEPR	Public Health Emergency Preparedness and Response
PHL	Public Health Labs
PHIMS	Public Health Issues Management System
PHIN	Public Health Information Network
PHPPPO	Public Health Practice Program Office (CDC)
PHS	Public Health Service
PHTN	Public Health Training Network
PIR	Priority Intelligence Requirements
PIO	Public Information Officer
PIP	Partners In Protection
PNR	Passenger Name Record
PNWER	Pacific Northwest Economic Region
POE	Port of Entry
POD	Port of Debarkation
PODO	Press Office Duty Officer
POLLREP	Pollution Report
PPA	Principal Planning Agent
PPC	Prevention and Preparedness Council
PPE	Personal Protective Equipment
PSA	Public Safety Announcement
PSAP	Public Safety Answering Point
PSCC	Public Safety Coordinating Council
PSC	Public Safety Communications
PSCDG	Primary State Core Decision Group
PSWAC	Public Safety Wireless Advisory Committee
PSWN	Public Safety Wireless Network
PTE	Potential Threat Element
PVMS	Prophylaxis and Vaccine Management System
PW	Public Works
PWR	Pressurized Water Reactor
R	Roentgen
RAD	Risk Assessment Division
RAIN	King County Regional Automated Information Network
RAP	Radiological Assistance Program (DOE)
RAPTR	Radio Analysis Prediction Tool Repository
RACES	Radio Amateur Civil Emergency Services
Rad	Radiological Absorbed Dose
RCECC	Regional Communications and Emergency Coordination Center
RCP	Regional Contingency Plan
RDD	Radiological Dispersal Devices
REAC/TS	Radiation Emergency Assistance Center/Training Site (DOE)
RERT	Radiological Emergency Response Team (EPA)
RFI	Request for Information
RFID	Radio Frequency Identification Cards
RHSCD	Regional Homeland Security Coordination Districts (WA State)
RISS	Regional Information Sharing System
ROC	Regional Operations Center (FEMA)
ROSS	Resource Ordering and Status System
RPA	Regional Planning Agent
RRIS	Rapid Response Information System (FEMA)
RRT	Regional Response Team

RRTF	Washington State Recovery and Restoration Task Force
RTF	Response Task Force (DOD)
RQ	Reportable Quantity
SAA	State Administrative Agency (Grants)
SAC	Special Agent in Charge (FBI)
SCBA	Self Contained Breathing Apparatus
SAR	Search and Rescue
SARDA	State and Regional Disaster Airlift Plans
SCBA	Self-Contained Breathing Apparatus
SCI	State Critical Infrastructure
SCIF	Sensitive Compartmented Information Facility
SCM	Survivable Crisis Management
SCO	State Coordinating Officer
SEB	Staphylococcus Entreotoxin B (a tox)
SEL	Standardized Equipment List
SENTRI	Secure Electronic Network for Traveler Rapid Inspection
SEVIS	Student and Exchange Visitor Information System
SERC	State Emergency Response Commission
SERRP	State Emergency Response and Recovery Plan
SGSGP	State Homeland Security Grant Program
SIEC	State Interoperability Executive Committee
SIOC	Strategic Information Operations Center (FBI)
SITREP	Situation Report
SGSGP	State Homeland Security Grant Program
SHSAS	State Homeland Security Assessment and Strategy Program
SHSP	State Homeland Security Program
SHSS	State Homeland Security Strategies
SIPRNET	Secure Internet Protocol Routing Network
SL	State and Local Government Representative
SLA	State and Local Assistance
SLPS	State and Local Programs and Support Directorate (FEMA)
SME	Subject Matter Expert
SOLAS	International Convention Act for the Safety of Life As Sea (1974)
SNS	Strategic National Stockpile
SOP	Standard Operating Procedures
SPOC	Single Point of Contact (Grant Review)
SRO	School Resource Officers
SSCDG	Secondary State Core Decision Group
S&T	Science and Technology
START	Scientific and Technical Analysis and Response Team
STISAC	Surface Transportation Information Sharing and Analysis Center
STRACNET	Strategic Rail Corridor Network
SWAT	Special Weapons and Tactics
SWO	Senior Watch Officer
TARU	Technical Advisory Response Unit
TAT	Technical Assistance Team
TC	Trauma Care
TCP	Transmission Control Protocol
TCV	Total Containment Vessel
TEA	Threat Environment Assessment
TEDE	Total Effective Dose Equivalent
TEU	Technical Escort Unit (U.S. Army)
TIA	Terrorist Incident Annex
TIIAP	Telecommunications and Information Infrastructure Assistance Program
TIP	Department of State Terrorist Interdiction Program
TIPS	Terrorism Information and Preventive Systems
TLD	Thermoluminescent Dosimeter
TMSARM	Transportation Security Administration Maritime Self-Assessment Risk Model
TSA	Transportation Security Administration

TSC	U.S. Terrorist Screening Center
TSWG	Technical Support Working Group
TSOB	Transportation Security Oversight Board
TTIC	Terrorist Threat Integration Center
TWIC	Transportation Worker Identification Card
TWOV	Transit Without Visa Program
UA	Urban Area (UASI)
UACG	Urban Area Core Group (UASI)
UAWG	Urban Area Working Group (UASI)
UASI	Urban Area Security Initiative
UC	Unified Command
UC/IC	Unified Command/Incident Command
UCR	Uniform Crime Reports
UCS	Unified Command System
USAR	Urban Search and Rescue
USFA	United States Fire Administration (FEMA)
USCG	United States Coast Guard
USRT	Urban Search and Rescue Team (FEMA)
USSS	United States Secret Service
U.S. VISIT	U.S. Visitor and Immigrant Status Indication Technology System
VACIS	Vehicle and Cargo Inspection System
VEE	Venezuelan Equine Encephalitis (a viral agent)
VIPS	Volunteers in Police Service
VMI	Vendor Managed Inventory (SNS)
VX	A nerve agent
WAC	Washington Administrative Code
WACII	Washington State Criminal Intelligence Index
WACIRC	Washington Computer Incident Response Center
WACO	Washington Association of County Officials
WADDL	Washington Animal Disease Diagnostic Laboratory
WAJAC	Washington Joint Analytical Center
WAEMD	Washington State Emergency Management Division
WAMA	Washington Airport Managers Association
WA SECURES	Washington State Electronic Communications and Urgent Response Exchange System
WASERC	Washington State Emergency Response Commission
WASPC	Washington Association of Sheriffs and Police Chiefs
WAPHL	Washington State Public Health Laboratories
WAVOAD	Washington Volunteer Organizations Active in Disasters
WCCMA	Washington City/County Management Association
WCIT	Washington Council on International Trade
WCNCS	Washington Commission for National & Community Services.
WEDSS	Washington Electronic Disease Surveillance System
WEIC	Washington Emergency Information Center
WMD	Weapons of Mass Destruction
WMD – CST	Weapons of Mass Destruction Civil Support Teams
WPC	Washington Poison Center
WPPA	Washington Public Ports Association
WSAC	Washington State Association of Counties
WSAFC	Washington State Association of Fire Chiefs
WSALPHO	Washington State Assoc. of Local Public Health Officials
WSDA	Washington State Department of Agriculture
WSDOE	Washington State Department of Ecology
WSDOH	Washington State Department of Health
WSEMA	Washington State Emergency Management Association
WSPHA	Washington State Public Health Association
WSDOT	Washington State Department of Transportation
WSHA	Washington State Hospital Association
WSP	Washington State Patrol
WUTC	Washington Utilities and Transportation Commission

APPENDIX F - REFERENCES

- National Strategy for Homeland Security – July 2002. http://www.whitehouse.gov/homeland/book/

- National Security Strategy of the United States – September 2002 http://www.whitehouse.gov/nsc/nss.html

- National Strategy to Combat Weapons of Mass Destruction – December 2002. http://www.whitehouse.gov/news/releases/2002/12/WMDStrategy.pdf

- National Strategy for Combating Terrorism – February 2003 http://www.whitehouse.gov/news/releases/2003/02/20030214-7.html

- National Strategy for Physical Protection of Critical Infrastructures and Key Assets – Feb 2003 http://www.whitehouse.gov/pcipb/physical.html

- National Strategy to Secure Cyberspace – February 2003 http://www.whitehouse.gov/news/releases/2003/02/20030214-7.html

- The Office for Domestic Preparedness Guidelines For Homeland Security Prevention and Deterrence – June 2003 http://www.ojp.usdoj.gov/odp/docs/ODPPrev1.pdf

- NSPD – 23: National Policy on Ballistic Missile Defense – December 02 http://www.fas.org/irp/offdocs/nspd/nspd-23.htm

- NSPD – 62: Protection Against Unconventional Threats to the Homeland and Americans Overseas – May 98 http://www.fas.org/irp/offdocs/pdd-62.htm

- NSPD – 63: Critical Infrastructure Protection – May 98 http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

- PDD/NSTC-5: Guidelines for Federal Laboratory Reform – September 1995 http://www.fas.org/irp/offdocs/pdd5status-a.html

- PDD/NSTC-7: Threat of Emerging and Re-Emerging Infectious Diseases: Jun 96 http://www.fas.org/irp/offdocs/pdd_ntsc7.htm

- National Border Patrol Strategy – February 2003 http://www.immigration.gov/graphics/shared/lawenfor/bpatrol/strategy.htm

- National Drug Control Strategy – February 2003 http://www.whitehousedrugpolicy.gov/policy/ndcs.html

- Border Safety Initiative – February 2003 http://www.customs.ustreas.gov/xp/cgov/enforcement/border_patrol/safety_initiative.xml

- Border Coordination Initiative – June 2003. http://www.immigration.gov/graphics/shared/lawenfor/bmgmt/inspect/bciint.htm

- Presidential Decision Directive 63 Protecting America's Critical Infrastructure – May 98 http://www.fas.org/irp/offdocs/pdd-63.htm

- Presidential Directives for Homeland Security

  - HSPD 1 Organization and Operation of the Homeland Security Council – 29 Oct 01 http://www.whitehouse.gov/news/releases/2001/10/20011030-1.html

  - HSPD 2 Combating Terrorism Through Immigration Policies – 29 Oct 01 http://www.whitehouse.gov/news/releases/2001/10/20011030-2.html

  - HSPD 3 Homeland Security Advisory System – 11 March 02 http://www.whitehouse.gov/news/releases/2002/03/20020312-5.html

  - HSPD 4 National Strategy to Combat Weapons of Mass Destruction – 11 Dec 02 http://www.fas.org/irp/offdocs/nspd/nspd-17.html

  - HSPD 5 Management of Domestic Incidents – 28 Feb 03 http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html

  - HSPD 6 Integration and Use of Screening Information – 16 Sep 03 http://www.whitehouse.gov/news/releases/2003/09/20030916-5.html

  - HSPD 7 Critical Infrastructure Identification, Prioritization, and Protection – 17 Dec 03 http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html

  - HSPD 8 National Preparedness – 17 Dec 03 http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html

  - DoDD 3025.1 Military Support to Civil Authorities – January 1993 http://www.dtic.mil/whs/directives/corres/pdf/d30251_011593/d30251p.pdf

  - DoDD 3025.12 Military Assistance for Civil Disturbances – February 1994 http://www.dtic.mil/whs/directives/corres/pdf/d302512_020494/d302512p.pdf

  - DoDD 3025.15 Military Assistance to Civil Authorities – February 1997 http://www.cdmha.org/toolkit/cdmha-rltk/PUBLICATIONS/dodd3025_15.pdf

  - DoDD 3025.15 DoD Cooperation with Civilian Law Enforcement – with change 1 December 1989 http://www.dtic.mil/whs/directives/corres/pdf/d55257_012285/d55257p.pdf

  - DoDD 1330.5 American National Red Cross – August 1969 (updated Dec 1991) http://www.dtic.mil/whs/directives/corres/pdf/d13305wch4_081669/d13305p.pdf

  - DoDD 1100.20 Support and Services for Eligible Organizations and Activities Outside the Department of Defense – Jan 1997 http://www.dtic.mil/whs/directives/corres/pdf/d110020_013097/d110020p.pdf

  - DoDD 5100.78 United States Port Security Program – January 1986 http://www.dtic.mil/whs/directives/corres/pdf/d510078_082586/d510078p.pdf

  - DoDD 200.12 Antiterrorism/Force Protection (AT/FP) – April 1999 http://www.dtic.mil/whs/directives/corres/pdf/d510078_082586/d510078p.pdf

  - DoDD 3150.5 DoD Response to Improvised Nuclear Device (IND Incidents) – March 1987 http://www.dtic.mil/whs/directives/corres/html/31508.htm

  - Washington State Comprehensive Emergency Management Plan – May 2002 http://emd.wa.gov/3-map/a-p/cemp/01-cemp-idx.htm

  - Comprehensive Emergency Management Planning Guide – March 2003 http://emd.wa.gov/3-map/a-p/plan-guide/01-plan-guide-idx.htm

- Washington State Hazard Identification and Vulnerability Assessment – 2001 http://emd.wa.gov/3-map/a-p/hiva/03-hiva-director.htm

- Washington State Emergency Operations Plan (EOP) http://emd.wa.gov/6-rr/rr-forms-pubs/e-ops/eop/eop-idx.htm

- Guidelines for Implementation of the State of Washington Homeland Security Advisory System – March 2003 http://emd.wa.gov/site-general/wahsas/wa-hsas-idx.htm

- Emergency Management Assistance Compact http://emd.wa.gov/1-dir/emac/emac-2001.htm

- Washington State Recovery Plan http://emd.wa.gov/3-map/a-p/recoveryplan/recoveryplantoc.htm

- The National Guard Homeland Security Field Reference Guide – (Draft) 2003

- The White House Progress Report on the Global War on Terrorism – Sep 2003 http://www.whitehouse.gov/homeland/progress/

- Homeland Security in the State of Washington – A Baseline Report on the Activities of State and Local Governments – A Century Foundation Report – 2003 http://www.tcf.org/Publications/HomelandSecurity/stehr.pdf

- Chapter 38.52 Revised Code of Washington (RCW) The Washington State Legislature - Emergency Management http://www.leg.wa.gov/RCW/index.cfm?fuseaction=chapterdigest&chapter=38.52

- Title 118 Washington Administrative Code (WAC) Military Department (Emergency Management)http://www.leg.wa.gov/wac/index.cfm?fuseaction=title&title=118